

4

الهاكر الأخلاقي

التعداد (Enumeration)

By

Dr.Mohammed Sobhy Teba

Enumeration

https://www.facebook.com/tibea2004

CONTENTS

4.1 مفهوم التعداد (ENUMERATION CONCEPTS)

من أجل فهم أفضل لمفهوم التعداد، فلقد قسمنا هذه الوحدة إلى أقسام مختلفة. ويتناول كل قسم خدمات ومنافذ مختلفة لكي يتم تعدادها. قبل البدء بعملية التعداد الفعلي، سنناقش أولاً مفاهيم التعداد.
سوف يتناول هذا القسم ما هو التعداد وتقنيات التعداد، وخدمات ومنافذ تعداد.

ما هو التعدادWhat is Enumeration ؟

يتم تعريف التعداد (**Enumeration**) باعتباره عملية استخراج المعلومات مثل أسماء المستخدم، أسماء الالة، موارد الشبكة، المشاركات والخدمات من قبل النظام. في مرحلة التعداد، المهاجم يقوم بإنشاء اتصالات نشطة للنظام ويقوم بتوجيه الاستعلامات للحصول على مزيد من المعلومات حول النظام الهدف. المهاجم يستخدم المعلومات التي تم جمعها لتحديد الثغرات أو نقاط الضعف في منظومة الأمن ومن ثم يحاول استغلالها. تقنيات التعداد تجري في بيئة إنترانت. هذا يشمل إجراء اتصالات نشطة مع النظام الهدف. من الممكن أن يعثر المهاجم على **Remote IPC share**، مثل **IPC$** في ويندوز، والذي يمكن الاستعلام عنها باستخدام جلسة عمل فارغة (**null session**) والتي تسمح بتعداد المساهمات **shares** والحسابات **accounts**.
كنا قد أبرزنا في الوحدات السابقة كيفية ان المهاجم يقوم بجمع المعلومات اللازمة حول الهدف دون حقاً تعدى الحدود على الجانب الخطأ من الحاجز القانوني. يمكن تصنيف نوع المعلومات المذكورة بالمهاجمين إلى الفئات التالية:

المعلومات التي يتم تعدادها من قبل الدخلاء كالاتى:

- موارد الشبكة والاسهم(**Network resources and shares**) .
- أسماء المستخدمين والمجموعات(**Users and groups**) .
- جدول التوجيه (**routing table**).
- إعدادات التدقيق والخدمات (**Auditing and service settings**)
- أسماء آلة (**Machine names**)
- التطبيقات والبانر (**Applications and banners**)
- تفاصيل SNMP وDNS (**SNMP and DNS details**)

تقنيات التعدادTECHNIQUES FOR ENUMERATION

في عملية التعداد(**Enumeration process**) ، فان المهاجم يقوم بجمع البيانات مثل أسماء مستخدمي وجروبات الشبكة، جداول التوجيه (**routing table**)، ومعلومات بروتوكول إدارة الشبكة البسيطة (**SNMP**). هذه الوحدة تكشف السبل الممكنة للمهاجمين للقيام بعملية التعداد للشبكة المستهدفة، وما الاجراءات التي يمكن اتخاذها ضد هذه العملية.

فيما يلي تقنيات التعداد المختلفة التي يمكن استخدامها من قبل المهاجمين:

1- استخراج أسماء المستخدمين باستخدام معرفات البريد الإلكتروني (Extract user names using email IDs).
بشكل عام، كل معرف بريد إلكتروني (**email ID**) يحتوي على قسمين؛ واحد هو اسم المستخدم والآخر هو اسم الدومين. هيكل عنوان البريد الإلكتروني هو **username@domainname**. بالنظر مثلا الى عنوان البريد **abc@gmail.com**؛ في هذا البريد الإلكتروني فان "**abc**" (الحروف التي سبقت الرمز "@") هو اسم المستخدم و"**gmail.com**" (الحروف التي تلي الرمز "@") هو اسم الدومين.

2- استخراج المعلومات باستخدام كلمات السر الافتراضية (Extract information using the default passwords)
يوفر العديد من الموارد على الانترنت قوائم لكلمات السر الافتراضية المعينة من قبل الشركة المصنعة لمنتجاتها. غالبا ما ينسى المستخدمين من تغيير كلمات المرور الافتراضية المقدمة من قبل الشركة المصنعة أو المطورة للمنتج. وإذا قام المستخدمين بعدم تغيير كلمات المرور الخاصة بهم لفترات طويلة، فانه من الممكن بسهولة تعداد البيانات الخاصة بهم من قبل المهاجمين.

3- Brute force Active Directory
Microsoft Active Directory عرضه لنقطة ضعف عملية التعداد لاسم المستخدم في وقت التحقق من إدخال المستخدم. هذا هو نتيجة التصميم الخطأ في التطبيق. إذا تم تمكين ميزة '**logon hours**'، فان محاولات خدمة المصادقة (**authentication services**) سوف

ينتج عنها رسائل خطأ مختلفة. ان المهاجمون يأخذون هذه الميزة ويستغلون نقاط الضعف من اجل عملية تعداد أسماء المستخدمين الصحيحة. في حال نجاح المهاجم في الكشف عن أسماء المستخدمين الصالحة/الصحيحة، فانه يمكنه القيام بهجوم **Brute force** للكشف عن كلمات المرور الخاصة بكل منها.

4- استخراج أسماء المستخدمين باستخدام SNMP (Extract user names using SNMP)

يمكن للمهاجمين بسهولة تخمين **'string'** باستخدام **SNMP API** والتي من خلالها يتم استخراج أسم المستخدم المطلوب.

5- استخراج الجروب الذي ينتمي اليه المستخدمين من الويندوز (Extract user groups from Windows)

هذه سوف تقوم باستخراج حسابات المستخدمين من المجموعات المحددة وتخزين النتائج وأيضا التحقق من إذا كانت هذه الحسابات تنتمي للمجموعة أم لا.

6- Extract information using DNS Zone Transfer

DNS zone transfer يكشف الكثير من المعلومات القيمة عن المنطقة المعينة (**zone**) التي تطلبها. عندما يتم إرسال طلب نقل منطقة **DNS** (**Zone transfer DNS**) إلى ملقم **DNS**، فان الخادم يقوم بنقل سجلات **DNS** الذي تحتوي على المعلومات مثل نقل منطقة **DNS**. يمكن للمهاجم الحصول على معلومات قيمة عن طوبوغرافية الشبكة الداخلية الهدف باستخدام نقل منطقة **DNS** (**Zone transfer DNS**).

الخدمات والمنافذ التي يتم تعدادها SERVICES AND PORTS TO ENUMERATE

TCP 53: DNS ZONE TRANSFER

يعتمد **نقل منطقة DNS** (**DNS Zone transfer**) على المنفذ **53TCP** بدلا من **53 UDP**. إذاً إذا كان المنفذ **TCP 53** قيد الاستخدام فإن ذلك يعني أن عملية **نقل منطقة DNS** قيد العمل. بروتوكول **TCP** يساعد في الحفاظ على قاعدة بيانات **DNS** متناسقة بين ملقمات **DNS**. هذا الاتصال يظهر فقط بين خوادم **DNS**. خوادم **DNS** دائما تستخدم بروتوكول **TCP** لنقل المنطقة. تأسيس الاتصال بين ملقمات **DNS** يساعد في نقل بيانات المنطقة (**Zone data**) ويساعد ايضا كل من المصدر والوجهة لملقمات **DNS** لضمان اتساق البيانات بينهم عن طريق **TCP ACK**.

TCP 135: Microsoft RPC Endpoint Mapper

The RPC port 135 يستخدم في تطبيقات كل من العميل / الخادم لاستغلال خدمة الرسائل. لوقفه فسوف تحتاج إلى فلترة المنفذ 135 على مستوى جدار الحماية. عند محاولة الاتصال بالخدمة، فإنها سوف تذهب من خلال هذا المخطط لاكتشاف المكان الذي توجد فيه.

TCP 137: NetBIOS Name Service (NBNS)

NBNS، المعروف أيضا باسم **Windows Internet Name Service (WINS)** ، والتي توفر خدمة تحليل الأسماء لأجهزة الكمبيوتر التي تشغل**NetBIOS** . خوادم الاسماء **NETBIOS** يحتوى على قاعدة بيانات أسماء **NetBIOS** لأسماء المضيفين وعنوان **IP** المقابلة لأسماء المضيفين. وظيفة **NBNS** هي ان تتطابق عناوين **IP** مع أسماء **NetBIOS** والاستعلامات. خدمة الاسماء هي عادة أول خدمة تتعرض للهجوم.

TCP 139: NetBIOS Session Service (SMB over NetBIOS)

NetBIOS session service يستخدم في بناء وهدم الجلسات بين أجهزة الكمبيوتر المستخدمة **NetBIOS**. تقام الجلسات من خلال تبادل الحزم. جهاز الكمبيوتر الذي يقوم بإنشاء الجلسة (**sessions**) يحاول إجراء اتصال **TCP** إلى المنفذ **139** على الكمبيوتر الذي سوف يتم بدا الجلسة منه. إذا تم إجراء الاتصال، فان الكمبيوتر الذي أقام الجلسة يقوم بإرسال عبر الاتصال حزمة "**Session Request**" مع أسماء **NetBIOS** للتطبيق الذي أنشاء الجلسة واسماء **NetBIOS** الذي من خلاله تقام الجلسة. الكمبيوتر الاخر الذي سوف يقام الجلسة معه سوف يستجيب اما بـ (***Positive Session Response***)، والتي تعنى ان الجلسة يمكن إنشائها أو (***Negative Session Response***)، والتي تشير الى أنه لا يمكن تأسيس الجلسة.

TCP 445: SMB over TCP (Direct Host)

باستخدام اتصال **TCP** على المنفذ **445** يمكنك الولوج مباشرة الى شبكة **TCP/IP MS** دون المساعدة من طبقات **NetBIOS**. يمكنك فقط الحصول على هذه الخدمة في الإصدارات الأخيرة من ويندوز مثل **Windows2K/XP**.
مشاركة/تبادل الملفات في ***Windows2K/XP*** يمكن أن يتم من خلال البروتوكول **Server Message Block (SMB)**. يمكنك أيضا تشغيل **SMB** مباشرة عبر اتصال **TCP/IP** في **Windows2K/XP** دون استخدام مساعدة من طبقه اضافيه من **NetBIOS** والتي تستخدم المنفذ **445** من اجل هذا الغرض.

UDP 161: Simple Network Management protocol (SNMP)

يمكنك استخدام بروتوكول **SNMP** لمختلف الأجهزة والتطبيقات (بما في ذلك الجدران النارية والموجهات **routers**) لتواصل التسجيل وإدارة المعلومات مع تطبيقات الرصد عن بعد. عملاء **SNMP** يستخدموا المنفذ **UDP 161**؛ و**asynchronous traps** يتم استقبالها على المنفذ **162**.

TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)

يمكنك استخدام **LDAP** (***Lightweight Directory Access Protocol***) بروتوكول الإنترنت، وتجعله يستخدم ***MS Active Directory***، مثل قيام بعض برامج البريد الإلكتروني للبحث عن معلومات الاتصال من ملقم. كل من **Microsoft Exchange** و**NetMeeting** تقوم بتثبيت خادم **LDAP** على المنفذ الخاص بها.

TCP/UDP 3368: Global Catalog Service

يمكنك استخدام المنفذ **TCP 3368**، والذي يستخدم أحد البروتوكولات الرئيسية في TCP / IP على شبكات البروتوكول المهيأة للاتصال؛ فانه يتطلب أسلوب ثلاثي المصافحة لإقامة اتصال **end-to-end communications**. عندما يتم تعيين الاتصال عندها فقط يتم ارسال بيانات المستخدم، ويمكن أن يتم ارسالها ثنائية اتجاهي عبر الاتصال. **TCP** يضمن تسليم حزم البيانات على المنفذ **3368** في نفس الترتيب الذي تم إرسالها.
يمكنك استخدام المنفذ **UDP 3368** للاتصال الغير مضمونة. أنها توفر خدمة لا يمكن الاعتماد عليها ومخططات قد تصل مكررة، غير مرتبه، أو يحصل فقد للحزم دون سابق إنذار او خطأ. التدقيق والتصحيح ليس من الضروري القيام بها في التطبيق، ويتجنب العمليات الإضافية على مستوى واجهة الشبكة.
UDP (**User Datagram Protocol**) هو الحد الأدنى لبروتوكول طبقة النقل(**Transport Layer protocol**) . الأمثلة التي غالبا ما تستخدم **UDP** تتضمن (**VoIP voice over IP (VoIP)**)، **streaming media**، و**real-time multiplayer games**.

TCP 25: Simple Mail Transfer Protocol (SMTP)

SMTP يسمح بنقل البريد الإلكتروني عبر الإنترنت وعبر الشبكة المحلية. أنه يعمل على الخدمة المهيأ للاتصال التي يقدمها بروتوكول التحكم بالإرسال (**TCP**)، وأنه يستخدم المنفذ رقم 25. القيام باستخدام **Telnet** إلى المنفذ 25 على المضيف البعيد؛ يستخدم في بعض الأحيان في اختبار ملقم **SMTP** على النظام البعيد ولكن هنا يمكنك استخدام هذه التقنية لتوضيح كيف يتم تسليم البريد بين النظم.

NETBIOS ENUMERATION 4.2

حتى الآن، لقد ناقشنا مفاهيم التعداد والموارد التي تعطي معلومات قيمة من خلال التعداد؛ الآن حان الوقت لوضعها موضع التنفيذ. إذا كنت تحاول تعداد المعلومات من الشبكة المستهدفة، فأن **NetBIOS** هو المكان الأول من حيث يجب عليك محاولة استخراج أكبر قدر من المعلومات الممكنة.
يصف هذا القسم تعداد **NetBIOS** والمعلومات التي يمكن استخراجها من خلال التعداد، فضلا عن أدوات تعداد **NetBIOS**.

NETBIOS ENUMERATION

الخطوة الأولى لتعداد جهاز ويندوز هو الاستفادة من*NetBIOS API* . *NetBIOS*هو اختصار ل **Network Basic Input Output System** ، والذي تم تطويره من قبل شركة **IBM** بالتعاون مع**Sytek .** يعمل بشكل حميم مع بروتوكول الـ **TCP\IP** ليعطي إمكانية الاتصال عبر الشبكات، وطبعا وضعته ميكروسوفت لكي يتمكن الناس من وصل اجهزتهم والمشاركة في ملفاتها وفي الطابعة وهو ما يسمونه بـ "*Sharing*"، لقد تم تطوير "**NetBIOS**"على انه الـ"**API**" وهو اختصار لـ "**Application Programming Interface**"، وذلك لتسهيل الوصول للموارد الشبكة المحلية عن طريق برنامج العميل أي ما يسمى بـ**Sharing.** اسم **NetBIOS** هو عباره عن سلسلة أحرف **16 ASCII** فريدة من نوعها تستخدم لتحديد أجهزة الشبكة عبر **TCP/IP** ؛ حيث يستخدم 15 حرفا لاسم الجهاز والحرف 16 للخدمة أو اسم سجل النوع (**Name record type**) .

المهاجمين يستخدموا تعداد NetBIOS للحصول على الاتي:

- قائمة أجهزة الكمبيوتر التي تندرج تحت الدومين ومشاركتهم (**Shares**) بالنسبة للمضيفين على الشبكة.
- السياسات وكلمات السر(**Policies and passwords**) .

إذا وجد المهاجم ويندوز **OS** مع المنفذ **139 مفتوحا**، فانه سوف يكون مهتما بفحص ما هي الموارد التي يمكن الوصول إليها، أو رؤيتها، على النظام البعيد. ولكن، لتعداد أسماء **NetBIOS**، في النظام البعيد فيجب تمكين **file and printer sharing**. باستخدام هذه التقنيات، يمكن للمهاجم إطلاق نوعين من الهجمات على الكمبيوتر البعيد الذي يملك **NetBIOS**.
المهاجم يمكنه أن يختار القراءة/الكتابة على نظام الكمبيوتر البعيد، وهذا يتوقف على مدى توافر المشاركة (**Share**)، أو إطلاق هجمة الحرمان من الخدمة (**denial of services**).
العديد من مزودي خدمات الإنترنت يقوموا الان بحجب منافذ **NetBIOS** في البنية التحتية الأساسية، وذلك حتى يفرغوا من الهجوم الموجه عبر الإنترنت. أقول هذا، ان في اختبارات الاختراق الداخلية، غالبا ما تواجه ويندوز NT، ويندوز 2000، أو خوادم لينكس سامبا التي لا تزال عرضة لهذا النوع من أساليب التعداد.
ملحوظه:NetBIOS لا يدعم IPv6.

NetBIOS Name List

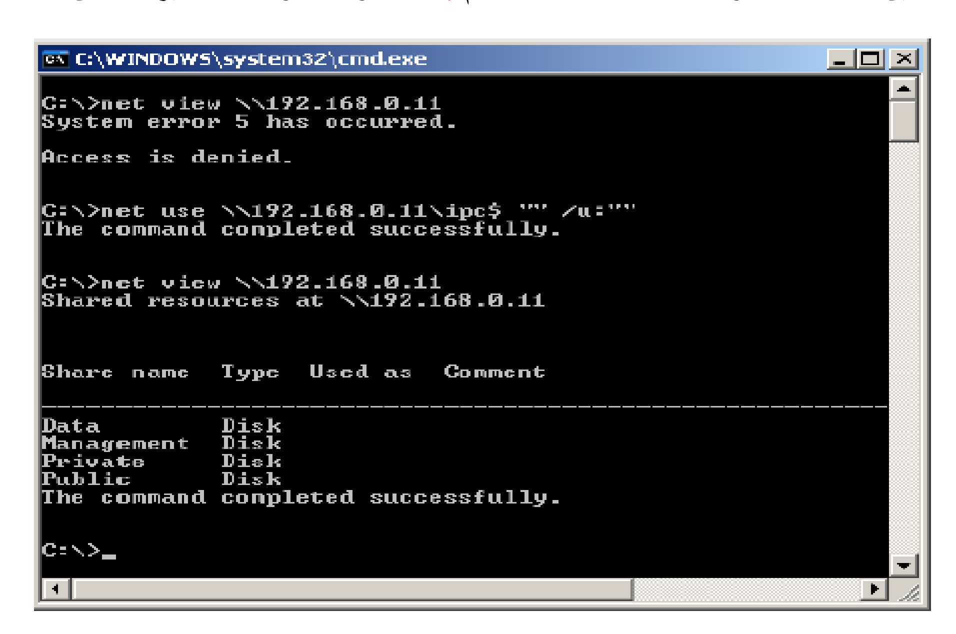
Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the PDC for that domain

تعمل NetBIOS على البورتات التالية:

137 netbios name
138 netbios datagram
139 netbios session

NULL SESSIONS

Null Session هو جلسة عمل **NetBIOS** غير مصادقه (**unauthenticated**) بين جهازي كمبيوتر. توجد هذه الميزة للسماح للات للحصول على قوائم الاستعراض من خوادم **Microsoft** الأخرى من غير مصادقه (**without authentication**). هذه الميزة تسمح أيضا للقراصنة الحصول على كميات ضخمة من المعلومات حول الجهاز من غير مصادقه (**without authentication**)، مثل سياسات كلمة السر، أسماء المستخدمين، أسماء المجموعة، أسماء الآلة، المستخدم و**SID**، وهكذا. وأفضل تفسير ذلك من خلال المثال التالي:



بعد إنشاء **Null session** يدويا، فان المهاجم يمكنه كشف قائمة المساهمات/المشاركات لكمبيوتر الضحية بالنسبة للمضيفين. لاحظ أن إنشاء **Null Session** يتم تعطيله في ويندوز إكس بي و2003 بشكل افتراضي. لمزيد من المعلومات حول **Null Session** وبروتوكول **NetBIOS**، يرجى زيارة الاتي:

http://en.wikipedia.org/wiki/NetBIOS
http://www.securityfriday.com/Topics/winxp2.html
http://www.securityfriday.com/Topics/restrictanonymous.html

SCANNING FOR THE NETBIOS SERVICE

يوجد العديد من الأدوات التي تتوفر لمساعدتك في تحديد أجهزة الكمبيوتر التي تشغل خدمات **NetBIOS** (تبادل الملفات في الويندوز (**Windows File Sharing**) مثل **nbtscan** و **smbserverscan** و **nbtstat**.

- **nbtstat**

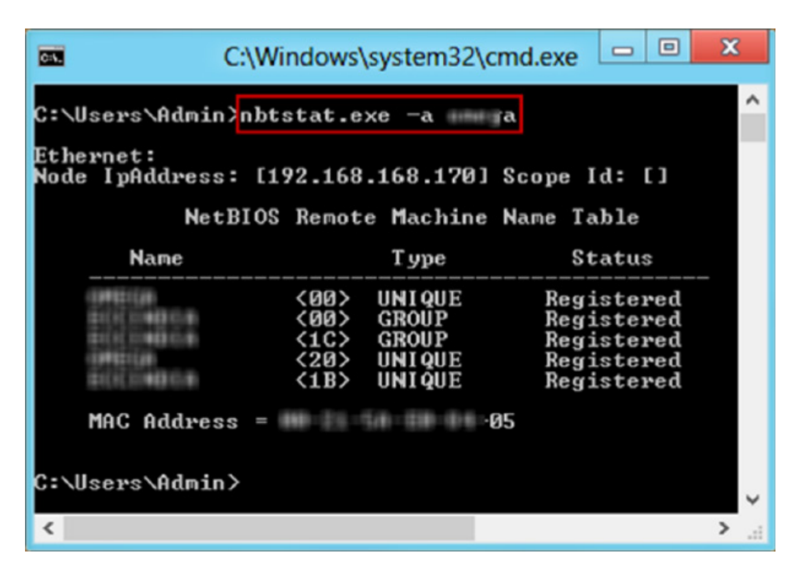
Nbtstat هي اداه لنظام التشغيل ويندوز تقوم بعرض إحصائيات البروتوكول **NetBIOS** عبر **TCP/IP** (**NetBT**) أو أسماء جداول **NetBIOS** لكل من الكمبيوتر المحلي وأجهزة الكمبيوتر عن بعد (**NetBIOS name tables**) ، واسم ذاكرة التخزين المؤقت **NetBIOS** (**NetBIOS name cache**). **Nbtstat** يسمح التحديث لذاكرة التخزين المؤقت **NetBIOS** و الأسماء المسجلين من قبل **WINS** (**Windows Internet Name Service**).عند الاستخدام الامر **nbtstat** بدون أي معاملات في سطر الأوامر في **command prompt**، فانه يعرض المساعدة المتعلقة به.

لتشغيل الأمر nbtstat.exe كالاتى:

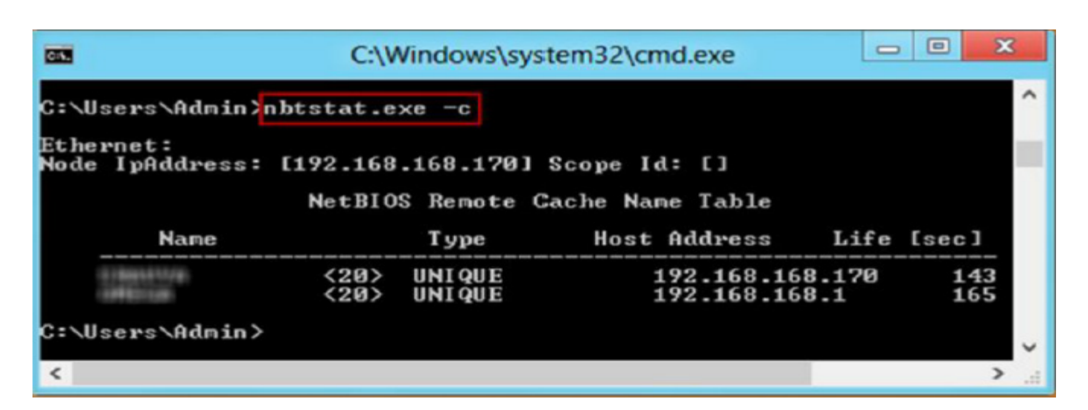
nbtstat.exe©-a©<NetBIOS Name of remote machine\IP of remote machine>

وذلك للحصول على اسم الجدول **NetBIOS** للكمبيوتر البعيد(**NetBIOS name tables**) .



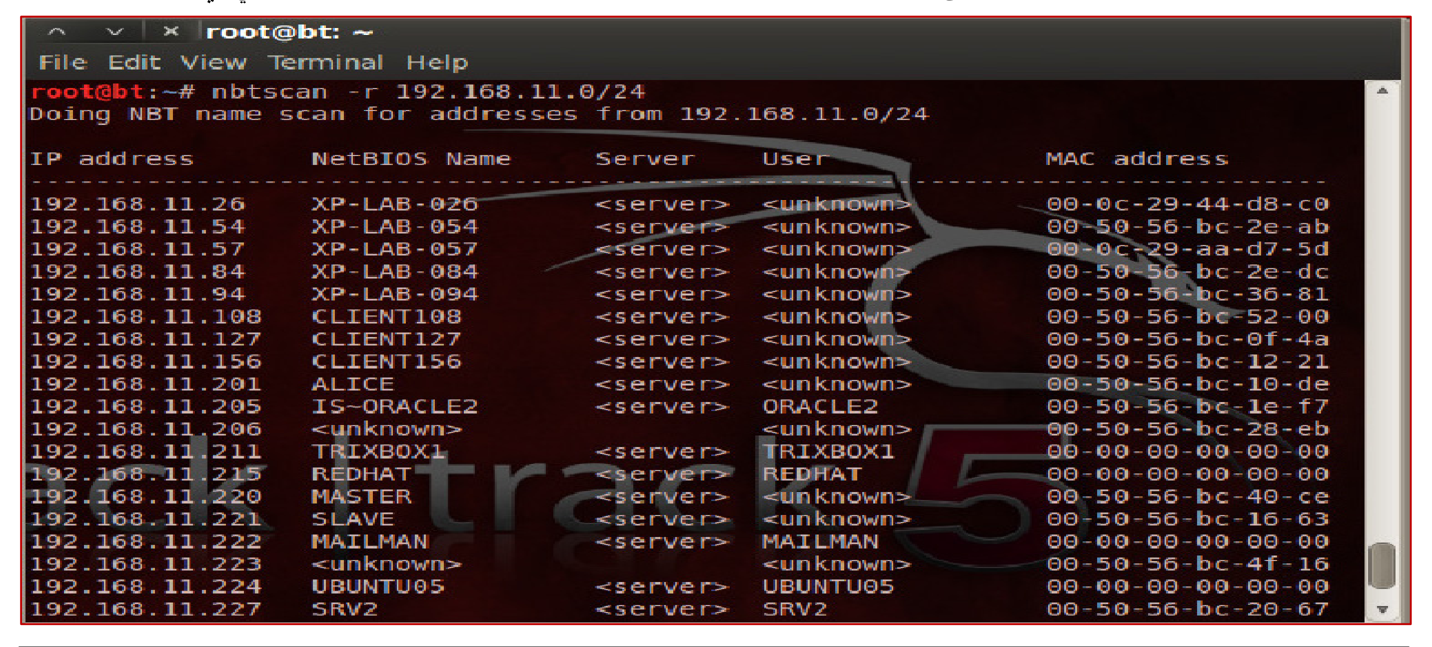


قم بتشغيل الامر **nbtstat** "**nbstat.exe -c**" لعرض محتويات ذاكرة التخزين المؤقت **NetBIOS**، جدول أسماء **NetBIOS**، وعناوين **IP** التي تم حلها(**resolved IP**) .



- **nbtscan**

Nbtscan اداه خاصه بنظام التشغيل لينكس, قادرة على تحديد الأجهزة على الشبكة الفرعية المحددة التي تقوم بتشغيل ***NetBIOS***. هذه الأداة يمكن أن تستعمل لفحص عناوين ال **IP** وتعطيك الأداة معلومات أو ناتج فيه عنوان الجهاز الضحية واسم المستخدم للجهاز وعنوان الماك أدرس ويمكن أيضا عرض جدول أسماء **NetBIOS** على جهاز الضحية إذا كان مصابا بهذه الثغرة، وهذه طبعا معلومات مهمة جدا في أي اختراق.



يمكنك أيضا عرض جدول أسماء NetBIOS التي على جهاز الضحية أو الهدف من خلال الأمر التالي

#nbtscan©-hv©192.168.16.70-80

```
root@jana:~# nbtscan -hv 192.168.16.70-80
Doing NBT name scan for addresses from 192.168.16.70-80

NetBIOS Name Table for Host 192.168.16.71:

Incomplete packet, 155 bytes long.
Name             Service          Type
----------------------------------------
JANA-TEBA        Workstation Service
JANA-TEBA        File Server Service
WORKGROUP        Domain Name

Adapter address: 00:1e:ec:af:fb:65
----------------------------------------
root@jana:~#
```

NetBIOS Enumeration Tool: Superscan

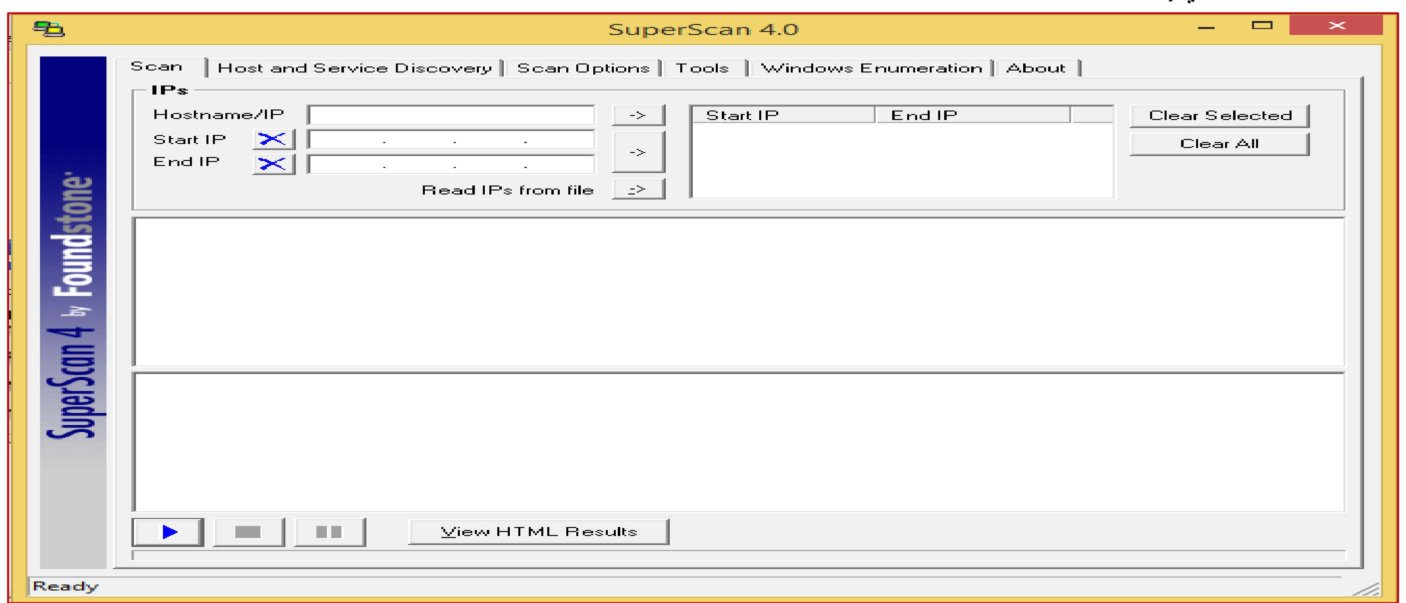
المصدر: http://www.mcaffe.com

Superscan هو أداة تقوم بفحص المنافذ (**Port scanner**) للاتصال القائم على **TCP**، **Pinger**، وترجمة اسم المضيف. يقوم بتنفيذ **Ping Swap** وفحص نطاق **IP** مع خاصية التعدد (**multithreading**)وتقنيات غير متزامنة.

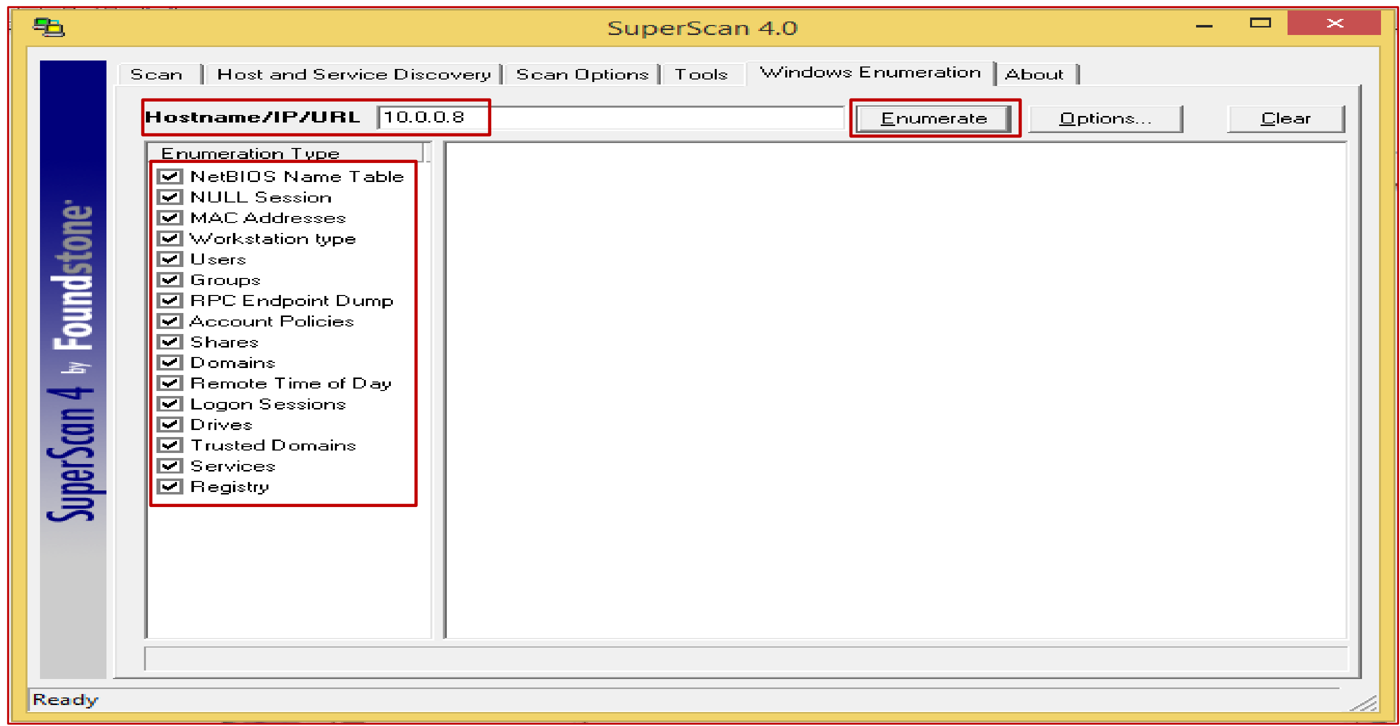
فيما يلي بعض ما يتميز به Superscan:

- **دعم لنطاقاتIP غير محدودة (Support for unlimited IP ranges)**
- **الكشف عن المضيف باستخدام أساليب ICMP متعددة (Host detection using multiple ICMP methods)**
- **فحص منافذ المصدر و TCP SYN و UDP (TCP SYN , UDP, and source port scanning)**
- **ترجمة اسم المضيف (Hostname resolving)**
- **الفحص العشوائي للمنافذ وعناوين IP (IP and port scan order randomization)**
- **القدرة على التعداد لمضيف الويندوز (Extensive Windows host enumeration capability)**
- **Extensive banner grabbing**
- **فحص منافذ المصدر (Source port scanning)**
- **انشاء تقرير بسيط بصيغة HTML (Simple HTML report generation)**

1- نجد ان هذا التطبيق لا يحتاج الى أي **Wizard** للتثبيت ولكن يتم تشغيله مباشرة عن طريق النقر فوق **SuperScan 4.0** فتظهر الشاشة التالية:

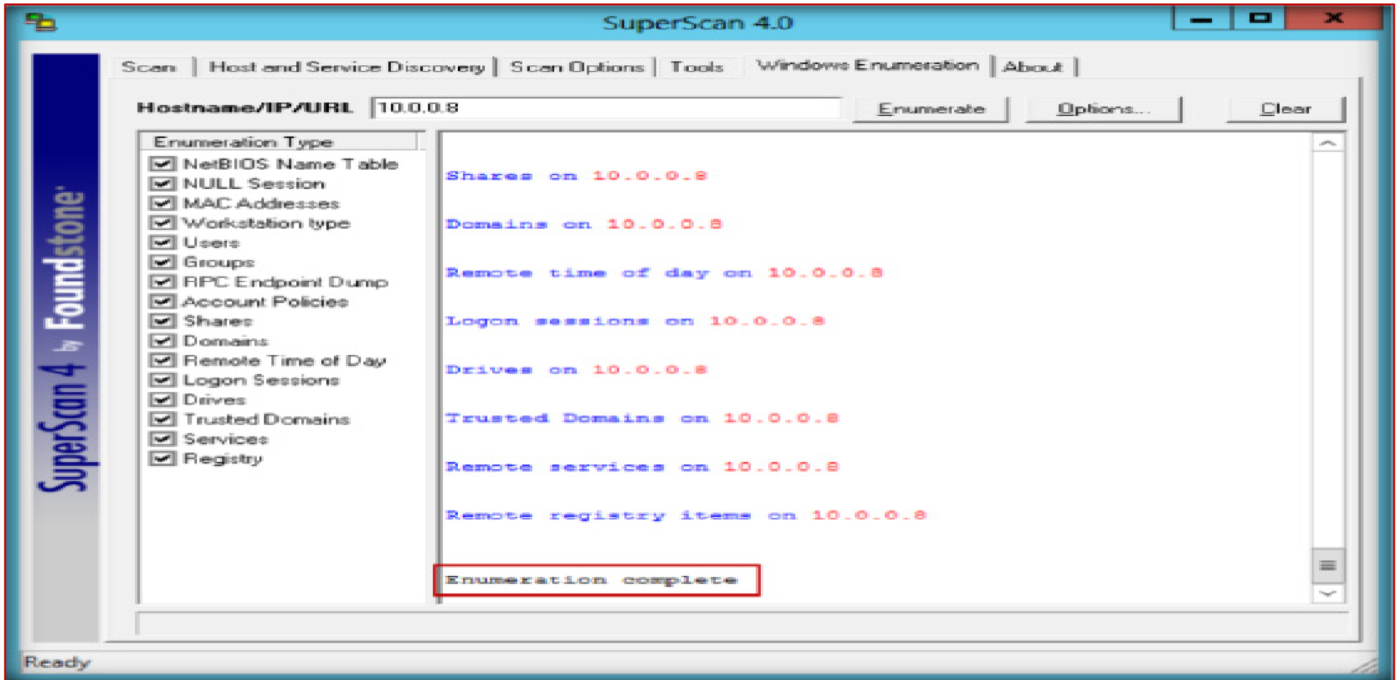


2- فلننظر الى شريط الأدوات العلوي والتي نجد انه يتكون من مجموعه من القوائم نقوم بالنقر على Windows Enumeration والتي تؤدى الى ظهور الشاشة التالية، والتي من خلالها نقوم بوضع اسم المضيف الضحية او عنوان IP الخاص به في الخانة المقابلة ل **Hostname/IP/URL**. من القائمة الموجودة في الجهة الايسر نختار منها نوع التعداد الذي تريده ثم بعد الانتهاء نضغط **Enumerate**.



ملحوظه: بداية من نظام التشغيل **windows xp services pack 2** قد ازالت تدعيم **raw sockets** والذي الان قد حد من عمل برنامج **SuperScan** وبرامج فحص الشبكة الأخرى. بعض الوظائف يمكن استرجاعها من خلال تشغيل **net stop Shared Access** في واجهة الأوامر (**command prompt**) الخاصة بويندوز قبل تشغيل **SuperScan**.

3- بعد الضغط على **Enumerate** يقوم بعملية التعداد ويظهر ناتج العملية في الجانب الأمين من الشاشة السابقة. انتظر قليلا حتى يتم الانتهاء من عملية التعداد ويعطى رسالة **Enumeration Complete** كالاتى:



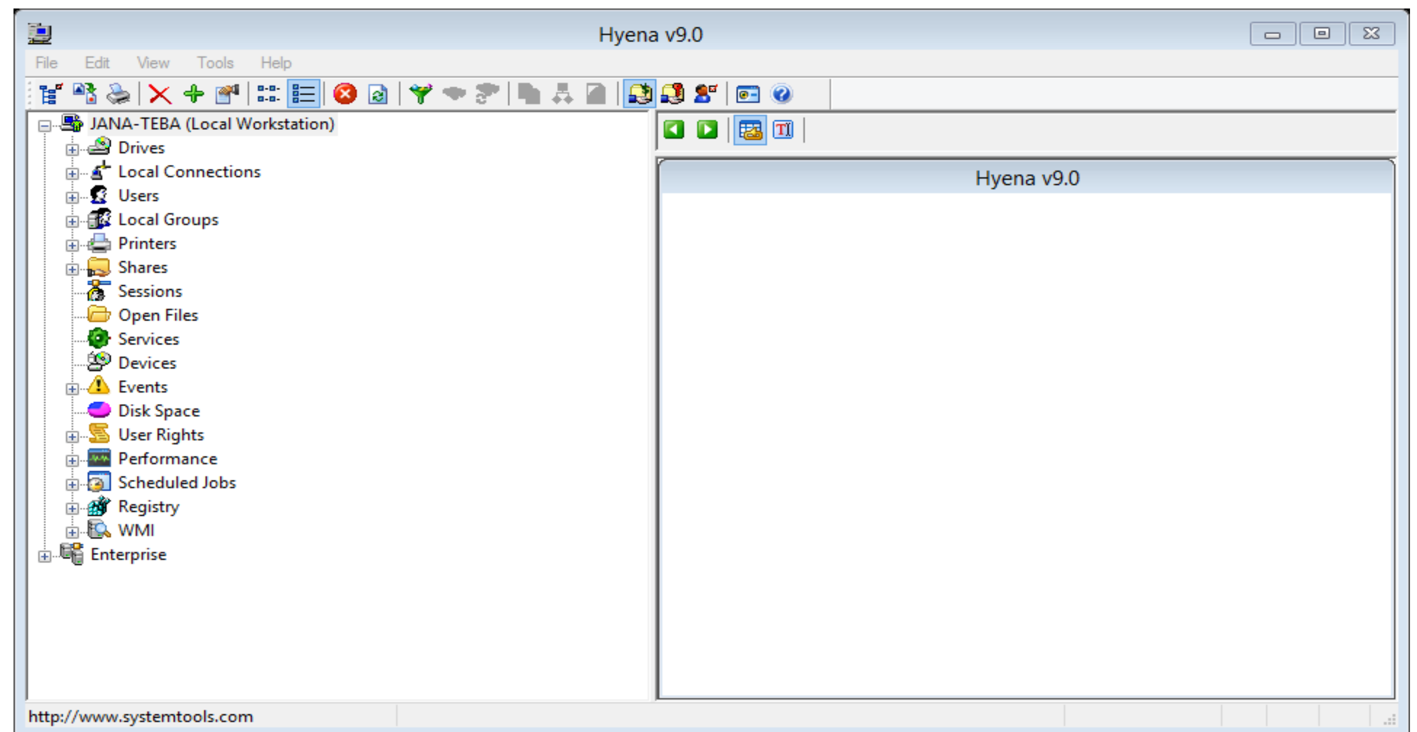
4- للقيام بعملية تعداد جديده لمضيف اخر فيجب أولا النقر فوق **Clear** الموجود بجانب **Enumerate**.

NetBIOS Enumeration Tool: HYENA

المصدر: http://www.systemtools.com

Hyena هو منتج ذات واجهة المستخدم الرسومية يستخدم لإدارة وتأمين أي نظام التشغيل ويندوز مثل ويندوزNT ، ويندوز 2000، ويندوز إكس بي, ويندوز فيستا، ويندوز 7، أو تثبيت ويندوز سيرفر 2003/2008. يستخدم واجهة اكسبلورر لجميع العمليات وإدارة المستخدمين والمجموعات (على الصعيدين المحلي والعالمي)، المساهمات/المشاركات، الدومين، الحواسيب، والخدمات، والأجهزة، الأحداث(**event**)، الملفات، الطابعات ومهام الطباعة، الجلسات (**session**)، الملفات المفتوحة، مساحة القرص، حقوق المستخدمين، الرسائل، التصدير، جدولة الوظائف، العمليات، والطباعة. فإنه يظهر المشاركات وأسماء دخول المستخدمين للخوادم الويندوز ووحدات تحكم الدومين (**Domain controller**). فإنه يعرض تمثيل رسومي للشبكة العميل على شبكة الإنترنت، خدمات مايكروسوفت ترمنال، وشبكة الويندوز.

1- لتثبيت التطبيق عن طريق اتباع **wizard** الخاص بعملية التثبيت، ثم بعد ذلك نقوم بالنقر على الأيقونة المعبرة عن التطبيق فيبدأ عمل البرنامج وتظهر الشاشة التالية:

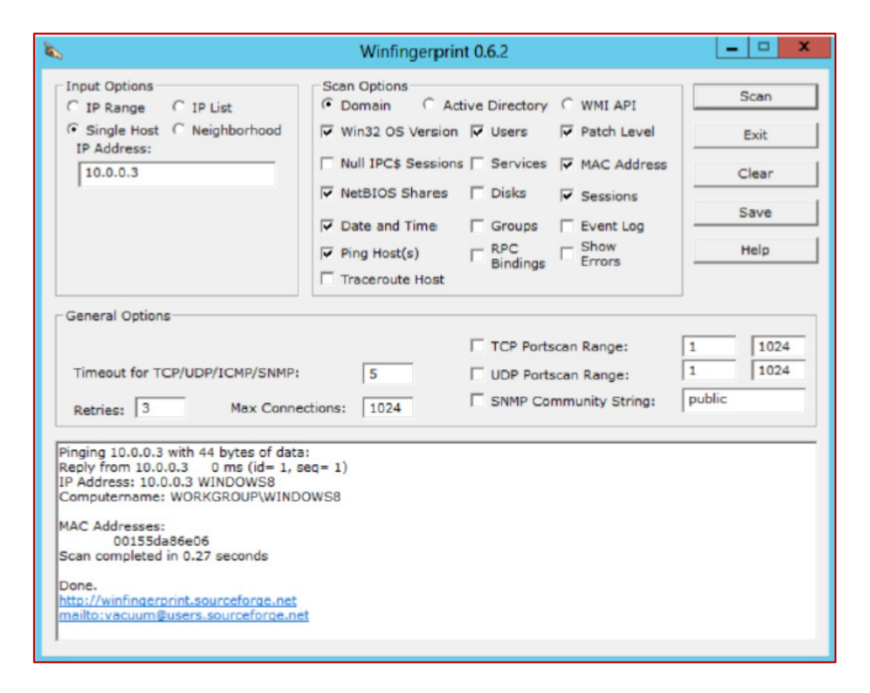


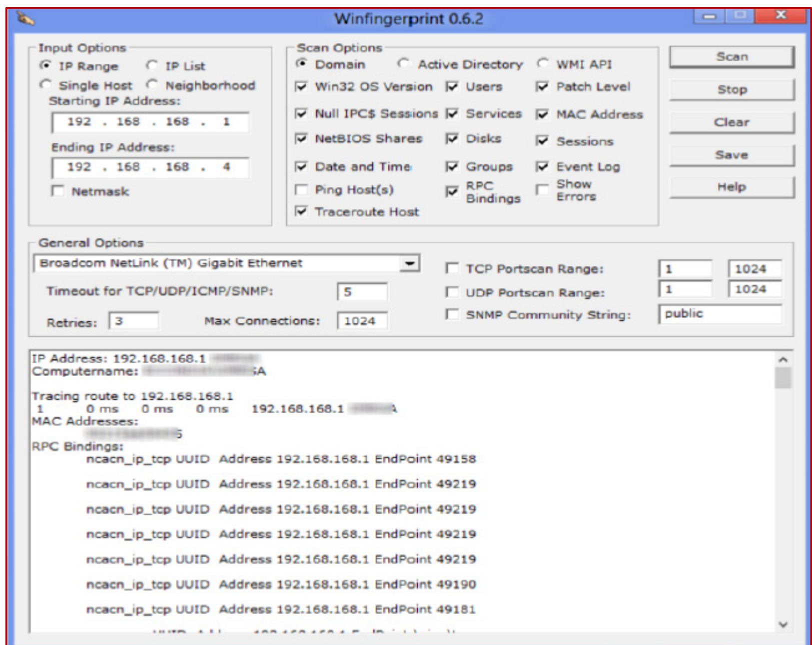
2- يمكن فحص الخدمات التي تعمل على النظام بالضغط على **Service** او الاحداث بالضغط على **Events** وهكذا كما ذكرنا سابقا على ما يقد التطبيق فعله. هذا التطبيق يشبه الى حد كبير **Computer management** الخاص بنظام التشغيل ويندوز.

NetBIOS Enumeration Tool: WinFingerprint

المصدر: http://www.winfingerprint.com

WinFingerprint هي أداة اداريه لفحص موارد الشبكة (**administrative network resource scanner**) والتي تسمح لك لفحص الأجهزة على شبكة الاتصال المحلية وإرجاع مختلف التفاصيل حول كل مضيف. وهذا يشمل مشاركات **NetBIOS**، معلومات القرص، الخدمات، المستخدمين، المجموعات، وأكثر من ذلك. يمكنك الاختيار لإجراء الفحص السلبي (**passive scan**) أو بشكل تفاعلي يستكشف مشاركات/مساهمات الشبكة، خريطة لمحركات أقراص الشبكة، تصفح مواقع HTTP/FTP وأكثر من ذلك. يمكن تشغيل الفحص على مضيف واحد أو على الشبكة بالكامل.



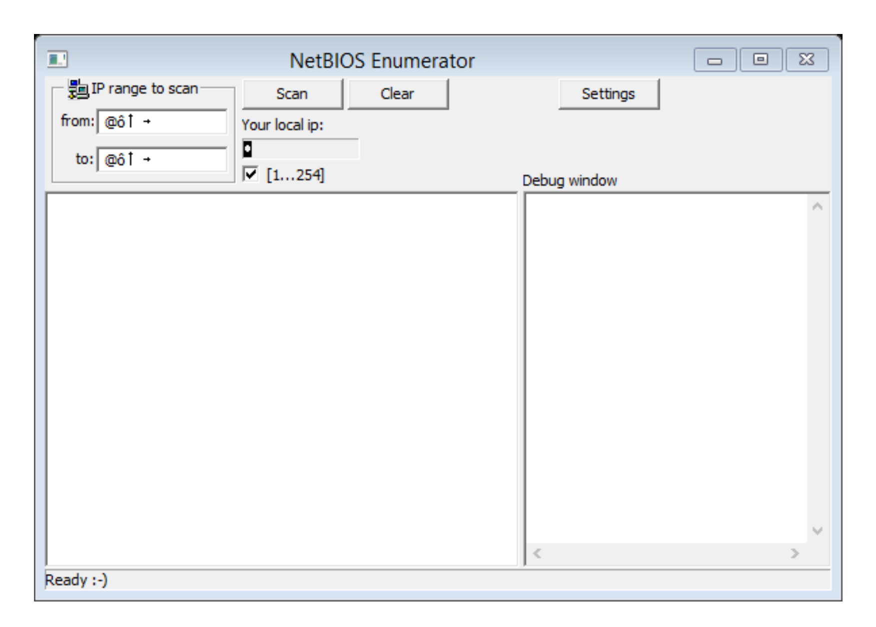


NetBIOS Enumeration Tool: NetBIOS Enumerator

المصدر: http://nbtenum.sourceforge.net

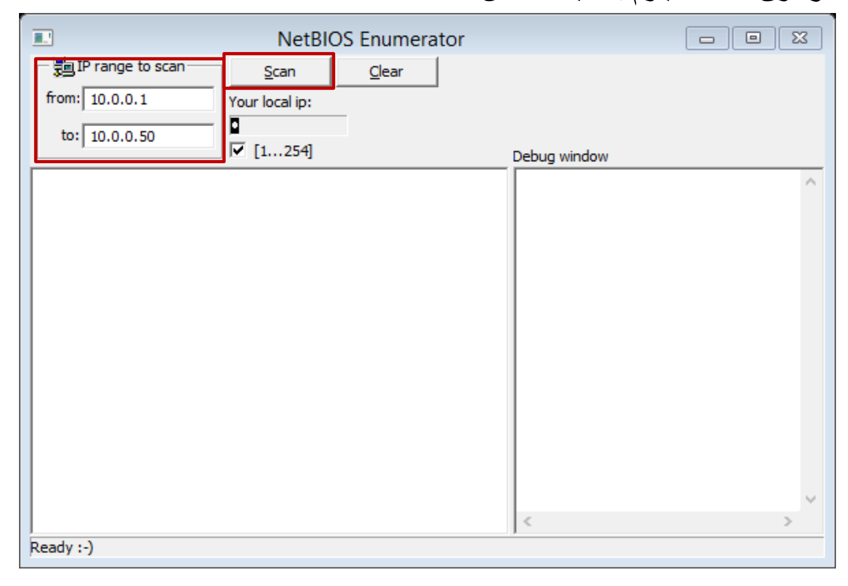
يوصى بهذا التطبيق عندما تريد تحديد كيفية استخدام دعم الشبكة عن بعد وكيفية التعامل مع بعض تقنيات الويب أخرى المثيرة للاهتمام، مثل **SMB**.

1- هذا التطبيق لا يحتاج الى عملية تثبيت. لتشغيله نقوم بالنقر المزدوج على NetBIOS Enumerater.exe حتى يبدا عمل البرنامج وتظهر الشاشة التالية:



2- في القائمة العلوية من شاشه التطبيق في القسم **IP range to scan** نقوم بإدخال نطاق عناوين **IP** الذي نريد ان نفحصه. بداية النطاق في الخانة المقابلة ل **from** ونهاية النطاق في الخانة المقابلة ل **to**.

3- بعد ادخال النطاق ننقر فوق **scan** ليقوم بعملية الفحص.



4- بعد النقر فوق **scan** سوف يقوم التطبيق بفحص نطاق عناوين **IP** الذي قمت بإدخاله ثم بعد الانتهاء سوف يقوم بعرض ناتج الفحص في الجانب الايسر من شاشة التطبيق.

5- لأداء فحص اخر يمكن ذلك من خلال النقر أولا فوق **clear** ثم ادخال نطاق العناوين **IP** الجديدة ثم النقر فوق **scan** والذي سوف يؤدى الفحص الجديد.

ملحوظه: عند القيام بفحص جديد فان ناتج الفحص القديم سوف يقوم التطبيق بازالته.

ENUMERATION USER ACCOUNT (تعداد حساب المستخدمين)

PSEXEC

المصدر: http://technet.microsoft.com/en-us/

PsExec هو أداة سطر الأوامر على عكس **telnet** وبرامج التحكم عن بعد **(Symantec's PC Anywhere)** والتي تمكنك من تنفيذ عمليات وبرامج وحدة التحكم على الأنظمة البعيدة، والتي تتطلب منك تثبيت برنامج العميل على الأنظمة البعيدة التي ترغب في الوصول

إليها. اما **PsExec** تمكنك من تنفيذ عمليات وبرامج وحدة التحكم على الأنظمة البعيدة، دون الحاجة الى تثبيت برنامج العميل يدويا على الأنظمة البعيدة التي ترغب في الوصول إليها.
عند استخدام حساب مستخدم معين، فان **PsExec** يمر وثائق التفويض في شكل واضح أي غير مشفر إلى محطة العمل عن بعد، وبالتالي من الممكن ان تصبح هذه البيانات في متناول أي شخص إذا قام بالاستماع الى هذا الاتصال.

PSFILE

المصدر: http://technet.microsoft.com/en-us/

PsFile هو أداة سطر الأوامر التي تظهر لائحة الملفات على النظام الذي يتم فتحه عن بعد، وايضا تسمح لك بغلق الملفات المفتوحة إما بالاسم أو معرف الملف. السلوك الافتراضي **PsFile** هو لسرد الملفات على النظام المحلي التي تكون مفتوحة من قبل الأنظمة البعيدة. كتابة الأمر متبوعا "**-**" يقوم بعرض المعلومات لبناء جملة الأمر.

PSGETSID

المصدر: http://technet.microsoft.com/en-us/

PsGetsid يسمح لك لترجمة **SIDs** إلى اسم العرض، والعكس بالعكس. يعمل على الحسابات المدمجة، حسابات الدومين، والحسابات المحلية. كما يسمح لك أيضا أن ترى **SIDs** من حسابات المستخدمين ويترجم **SID** إلى الاسم الذي يمثله وتعمل عبر الشبكة بحيث يمكنك الاستعلام عن **SIDs** عن بعد.

PSKILL

المصدر: http://technet.microsoft.com/en-us/

PsKill هي أداة قتل (**kill**) التي يمكن أن تقتل/تغلق العمليات على الأنظمة البعيدة وإنهاء العمليات على الكمبيوتر المحلي. لا تحتاج إلى تثبيت برنامج العميل على الكمبيوتر الهدف لاستخدام **PsKill** لإنهاء العملية البعيدة.

PSINFO

المصدر: http://technet.microsoft.com/en-us/

PsInfo هو أداة سطر الأوامر التي تجمع المعلومات الأساسية حول نظام ويندوز NT/2000 المحلية أو البعيدة، بما في ذلك نوع التثبيت، بناء النواة، سجل المنظمة والمالك، عدد المعالجات وانواعها, مقدار الذاكرة الفعلية، تاريخ تثبيت النظام، هل هو نسخة تجريبية، وتاريخ انتهاء الصلاحية.

PSLIST

المصدر: http://technet.microsoft.com/en-us/

PsList هو أداة سطر الأوامر التي يستخدمها المسؤولين لعرض معلومات حول عمليات وحدة المعالجة المركزية ومعلومات عن الذاكرة أو إحصاءات العمليات (**threads statistics**). الأدوات في مجموعات الموارد(**Resource kit**) ، **pstat** و **pmon**، تظهر لك أنواع مختلفة من البيانات ولكن فقط نقوم بعرض المعلومات المتعلقة بالعمليات على النظام الذي قامت بتشغيل الأدوات.

PSLOGGEDON

المصدر: http://technet.microsoft.com/en-us/

يمكنك تحديد من الذي يستخدم الموارد على الكمبيوتر المحلي الخاص بك مع الامر "**net**"، ومع ذلك، لا توجد وسيلة مدمجة في تحديد من يستخدم موارد كمبيوتر في الجهاز عن بعد. بالإضافة إلى ذلك، ويندوز **NT** لا يأتي مع أي من الأدوات لمعرفة من الذي قام بالتسجيل على

جهاز كمبيوتر، إما محليا أو عن بعد. **PsLoggedOn** هو برنامج صغير الذي يعرض كل من المستخدمين الذين قاموا بتسجيل الدخول إما على الكمبيوتر المحلي، أو عن بعد. إذا قمت بتحديد اسم المستخدم بدلا من جهاز كمبيوتر، **PsLoggedOn** يبحث في أجهزة الكمبيوتر في حي الشبكة ويخبرك إذا تم تسجيل دخول المستخدم حاليا.

يحدد **PsLoggedOn** من قام بتسجيل الدخول عن طريق فحص مفاتيح المندرجة تحت المفتاح **HKEY_USERS** في ملف **registry**.

PSLOGLIST

المصدر: http://technet.microsoft.com/en-us/

السلوك الافتراضي **PsLogList** هو إظهار محتويات سجل أحداث النظام (**System Event Log**) على الكمبيوتر المحلي، ويكون تنسيق الإخراج بطريقه بصريه لعرض سجل الأحداث. هو خيارات سطر الأوامر والذي يمكنك من عرض ملفات السجل (**logs**) على أجهزة كمبيوتر المختلفة، استخدم حساب مختلف لعرض السجل، أو أن يكون تنسيق الإخراج بطريقة (**string-search**).

PSPASSWD

المصدر: http://technet.microsoft.com/en-us/

PsPasswd هو الأداة التي تمكن المسؤول من إنشاء ملفات الباتش التي تعمل على تشغيل **PsPasswd** على شبكة من أجهزة الكمبيوتر لتغيير كلمة مرور المسؤول كجزء من الممارسات الأمنية القياسية.

PSSHUTDOWN

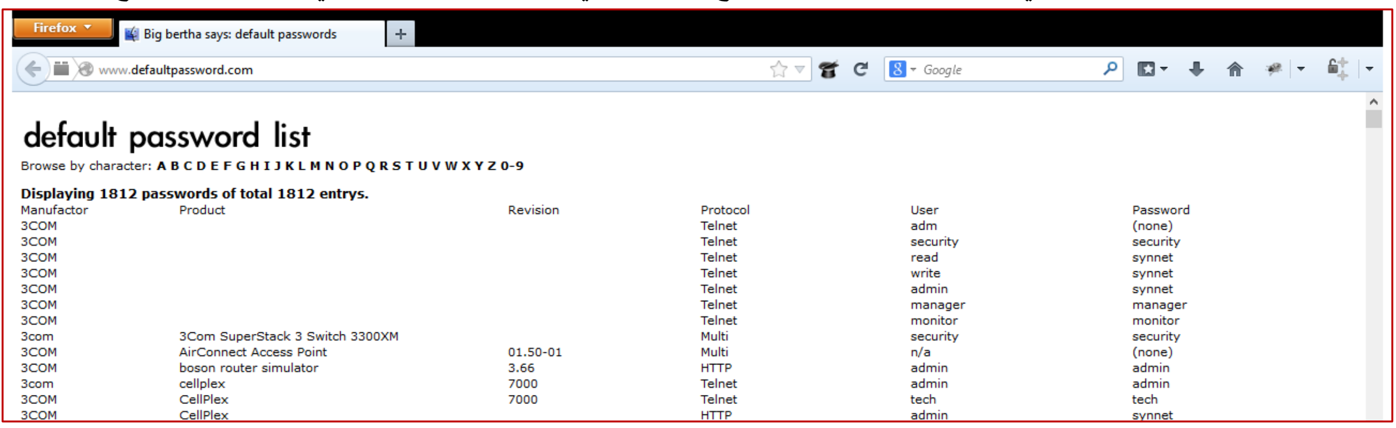
المصدر: http://technet.microsoft.com/en-us/

PsShutdown هو أداة سطر الأوامر التي تسمح لك بإغلاق جهاز الكمبيوتر موجود في الشبكة عن بعد. فإنه يمكن تسجيل الخروج للمستخدم قفل وحدة التحكم أو وحدة التحكم (يتطلب تأمين ويندوز 2000 أو أعلى). أنها لا تتطلب أي تثبيت يدوي من برنامج العميل.

ENUMERATE SYSTEMS USING DEFAULT PASSWORDS

المصدر: http://www.defaultpassword.com

الأجهزة مثل **switch**، **hub**، و**router**، عادة ما تأتي مع "كلمات السر الافتراضية". ليست فقط أجهزة الشبكة ولكن أيضا قد عدد قليل من التطبيقات المحلية والتطبيقات على شبكة الإنترنت بنيت مع كلمات السر الافتراضية. يتم توفير كلمات السر هذه من قبل البائعين أو مبرمجي التطبيق أثناء تطوير للمنتج. معظم المستخدمين يستخدموا هذه التطبيقات أو الأجهزة دون تغيير كلمات السر الافتراضية المقدمة من قبل البائع أو المبرمج. إذا لم تقم بتغيير كلمات المرور الافتراضية هذه، فإنك قد تكون في خطر بسبب قوائم كلمات السر الافتراضية للعديد من المنتجات والتطبيقات على شبكة الإنترنت. بمجرد الأمثلة على ذلك هو http://www.defaultpassword.com والتي توفر قائمة بكلمات المرور وتسجيلات الدخول الافتراضي للأجهزة المتصلة بالشبكة المشتركة. يتم تعيين تسجيلات الدخول وكلمات المرور الواردة في قاعدة البيانات هذه إما بشكل افتراضي عند تثبيت الأجهزة أو البرامج الأولى أو في بعض الحالات ضمنية في الأجهزة أو البرامج.



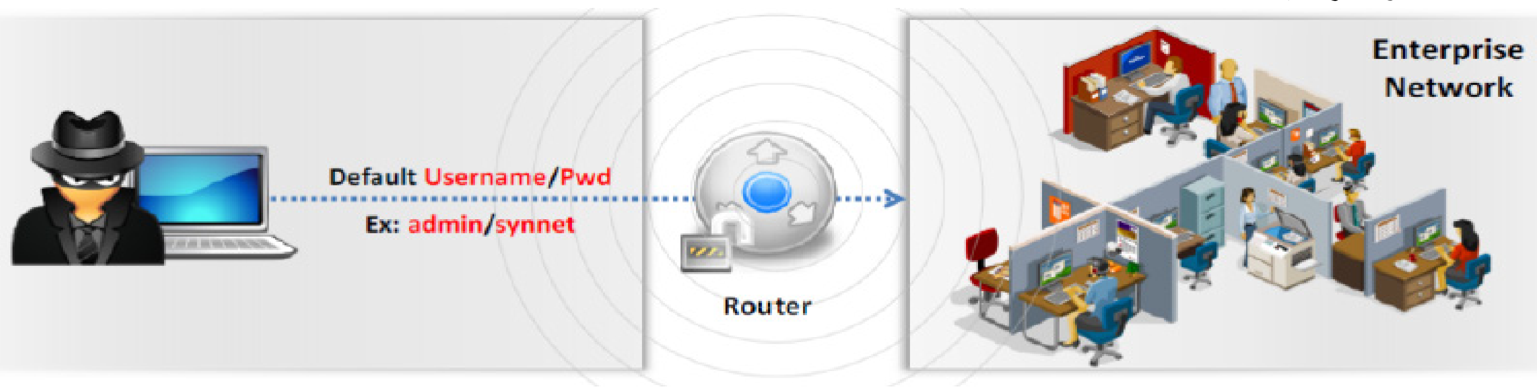
default password list

Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

Displaying 1812 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password
3COM			Telnet	adm	(none)
3COM			Telnet	security	security
3COM			Telnet	read	synnet
3COM			Telnet	write	synnet
3COM			Telnet	admin	synnet
3COM			Telnet	manager	manager
3COM			Telnet	monitor	monitor
3com	3Com SuperStack 3 Switch 3300XM		Multi	security	security
3COM	AirConnect Access Point	01.50-01	Multi	n/a	(none)
3COM	boson router simulator	3.66	HTTP	admin	admin
3com	cellplex	7000	Telnet	admin	admin
3COM	CellPlex	7000	Telnet	tech	tech
3COM	CellPlex		HTTP	admin	synnet

المهاجمون يستفادوا من كلمات السر الافتراضية هذه والموارد المتوفرة على الانترنت التي تقدم كلمات المرور الافتراضية لمختلف المنتجات والتطبيق. المهاجمين يقومون بالوصول الغير مصرح به إلى شبكة الكمبيوتر لمنظمة وموارد المعلومات باستخدام كلمات السر الشائعة والافتراضية.



ENUMERATING USERNAME/PASSWORD POLICIES

لتعداد معلومات المستخدم من جهاز ويندوز يسمح **null sessions**، يمكنك استخدام أدوات أكثر تخصصا في نظام التشغيل كالي مثل **samrdump** (نصي سكريبت بايثون)، أو **rpclient** المتاحة في كالي. والتي تعطيك كمية هائلة من المعلومات المثيرة للاهتمام:

```
root@bt:~# samrdump.py 192.168.2.102
Retrieving endpoint list from 192.168.2.102
Trying protocol 445/SMB...
Found domain(s):
 . 97DACBEC7CA4483
 . Builtin
Looking up users in domain 97DACBEC7CA4483
Found user: Administrator, uid = 500
Found user: Guest, uid = 501
```

SNMP ENUMERATIOM 4.3

يصف هذا القسم الأوامر يونيكس / لينكس التي يمكن استخدامها للتعداد وأدوات التعداد لينكس.

SNMP (Simple Network Management Protocol) Enumeration

أنا أعتبر أن بروتوكول **SNMP** بروتوكول مستضعف. لسنوات عدة قد أسيء فهمه على نطاق واسع. **SNMP** هو بروتوكول إدارة وغالبا ما يستخدم لرصد واعداد عن بعد الخوادم وأجهزة الشبكة. إذا كان **SNMP**، **MIB tree**، أو **OID**، غير مألوفين اليك فيمكنك التحقق من ويكيبيديا للحصول على مزيد من المعلومات:

http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

ما هو الـ SNMP وكيف يعمل وماهي إصداراته؟

في ظل الانفتاح الكبير على الانترنت وعلى الشبكات وزيادة نسبة الأجهزة التي تقوم بعملية أدارة الشبكات مثل الراوترات السويتشات وزيادة فعاليتها يوم بعد يوم وحتى يستطيع مهندسي الشبكات مراقبة أجهزتهم وطريقة أدائها فكان لا بد لهم من إيجاد بروتوكول خاص للمراقبة عن بعد يعطيهم بيانات دائمة لكفاءة عمل الأجهزة على الشبكة وبما فيها كفاءة عمل المعالج والرامات وكمية نقل البيانات ضمن الشبكة والكثير من خصائص المراقبة الهامة.

بروتوكول إدارة الشبكة البسيط **Simple Network Management Protocol (SNMP)** هو بروتوكولٌ للإدارة والصيانة صمّم خصيصاً للشبكات الحاسوبيّة وتجهيزات الشبكة الإفراديّة. تم البدا في تطوير بروتوكول الـ **SNMP** عام 1988 ليقوم بعملية المراقبة وهو

بروتوكول مطور من بروتوكول آخر تم تطويره عام 1987 أسمه **SGMP** أو **Simple Gateway Management Protocol** وجاء بعده بروتوكول آخر ظن الجميع انه سوف يحل مكان **SNMP** وهو **CMIP secure Common Management Information Protocol** لكن الأخير لم يدوم كثيرا كون الـ **SNMP** أثبت فعاليته بشكل أقوى على الساحة كونه يعمل على نطاقات واسعة وقابل للعمل مع جميع أنواع مكونات الشبكة (*Network component*). وكلاء **SNMP** (*SNMP agent*) يتم تشغيلها على شبكات **Windows** و **UNIX** على أجهزة الشبكات.

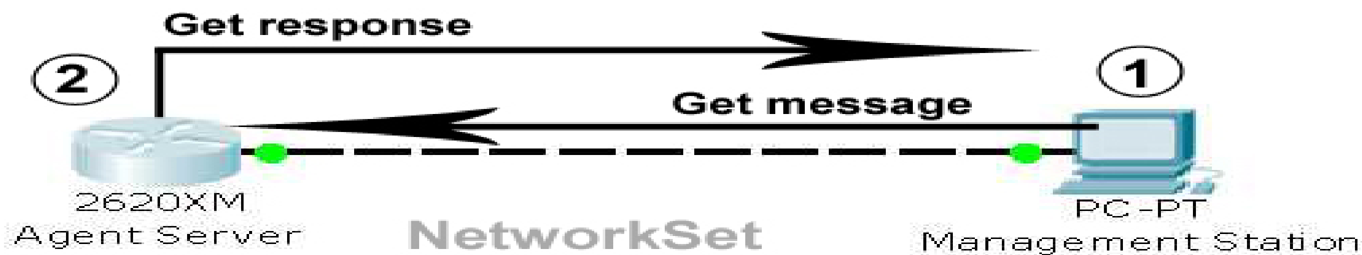
تعداد **SNMP** هو عملية تعداد لحسابات المستخدم والأجهزة على الكمبيوتر الهدف الذين يستخدموا **SNMP** . في الحقيقة بروتوكول الـ **SNMP** يقسم الى قسمين القسم الأول ويدعى **Agent** او السيرفر وهو هنا الجهاز المراد مراقبته مثل الروتر، السويتش، الطابعة الخ أما القسم الثاني **NMS (Network Management Station)** أو العميل وهو الجهاز الذي سوف يستلم البيانات من الـ**Agent** .

كيف يعمل الـ SNMP؟

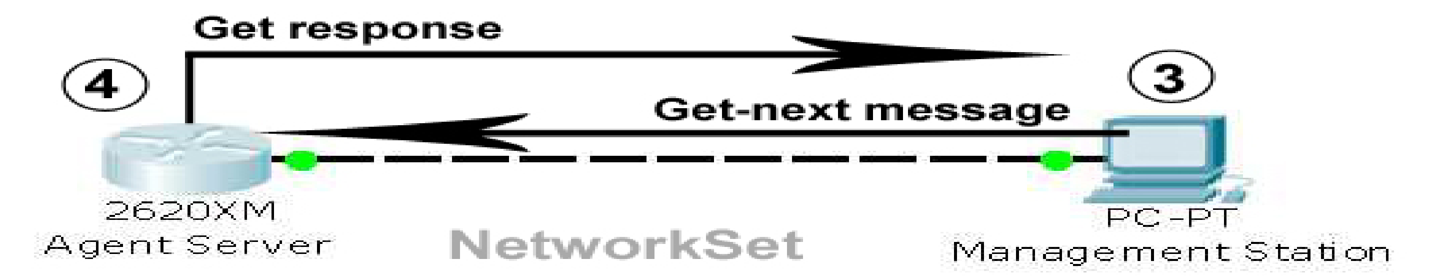
SNMP هو أحد بروتوكولات الطبقة السابعة **Application Layer** ويستخدم الـ **UDP/IP** للأرسال ومن خلال البورت 161 & 162.
هو بروتوكول **stateless**، وبالتالي فهو عرضة للخداع **IP** (**IP Spoofing**). يحتوي كل جهازٍ يدعم بروتوكول **SNMP** على قاعدة بياناتٍ تدعى **MIB** (قاعدة معلومات الإدارة Management Information Base). تحتوي قاعدة البيانات هذه على المعلومات التي يتم تجميعها أثناء عمل الجهاز. يمكن القول بأنّ بروتوكول **SNMP** يشكّل آليّة إرسال الطلبات واستقبال الردود عن معلومات الإدارة من العناصر الفعّالة في الشبكة. يستخدم خمس أنواع من الرسائل للتواصل بين السيرفر والعميل وهي

(**GET, GET-NEXT, GET-RESPONSE, SET, and TRAP**)

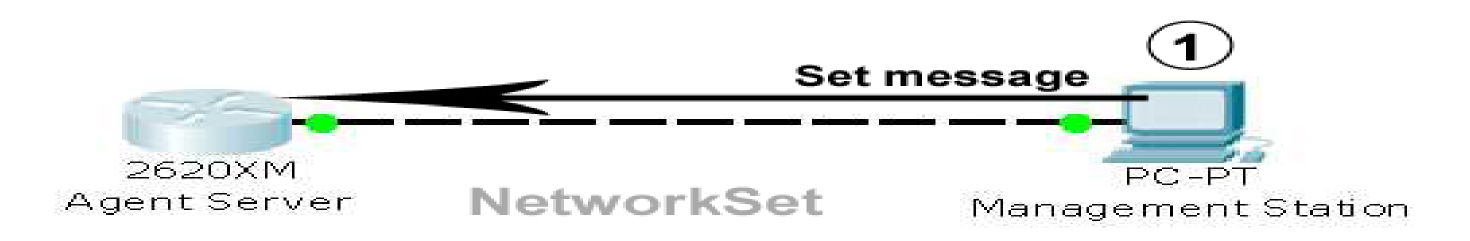
فعندما يريد العميل ان يبدأ المراقبة يقوم بأرسال **Get message** الى الـ **Agent** وهو بدوره يرسل المطلوب على شكل **Get-Response** كما نرى من الصورة القادمة.



كلا الطلبين والردود هي متغيرات الاعدادات التي يتم الوصول إليها من قبل برمجيات الوكيل(**Agent**). أما بالنسبة للرسالة **Get-Next** فهي عندما يريد أن يتابع عملية المراقبة ويرغب في الحصول على المزيد من المتغيرات.



رسالة الـ **Set** ترسل من قبل العميل لكي يطلب من الـ **Agent** شيء ما يتم تحديده في حال حدوث أي تغيير على السيرفر (تغيير قيمة).



ترسل أيضا الطلبات من **SNMP management station** لتعيين قيم لبعض المتغيرات. أما رسالة ال **Trap** ترسل من قبل الـ **Agent** في حال حدوث شيء ما في الجهاز المراقب مثلا توقف بورت عن العمل (Link Down/Up) أو إعادة التشغيل أو فشل الواجهة أو أي حدث غير طبيعي. هو في هذه الحالة يرسلها على البورت **162** بينما باقي الرسائل ترسل على البورت161.

SNMP يحتوي على اثنين من كلمات المرور التي يمكنك استخدامها للإعداد وكذلك للوصول إلى وكيل **SNMP** (**SNMP Agent**) من محطة الإدارة(**SNMP Management Station**) وهذه يطلق عليها **SNMP Community String**.
حيث يقوم العمل (***Management station***) بارسال الطلبات (**GET**) الى السيرفر (**Agent**) مع كلمة المرور (***Community String***) فاذا توافق كلمة المرور يتم ارسال الردود من قبل السيرفر (**Agent**) اما إذا لم يتوافق لن يتم ارسال أي شيء و هكذا.
ملحوظه: هذا النوع من كلمات المرور (**Community String**) يستخدم مع الإصدارات **SNMPv1** و **SNMPv2**. اما **SNMPv3** فتستخدم اسم المستخدم وكلمة السر في عملية المصادقة(**Authentication**).

كلمات السر الاثنين لـ SNMPهما:

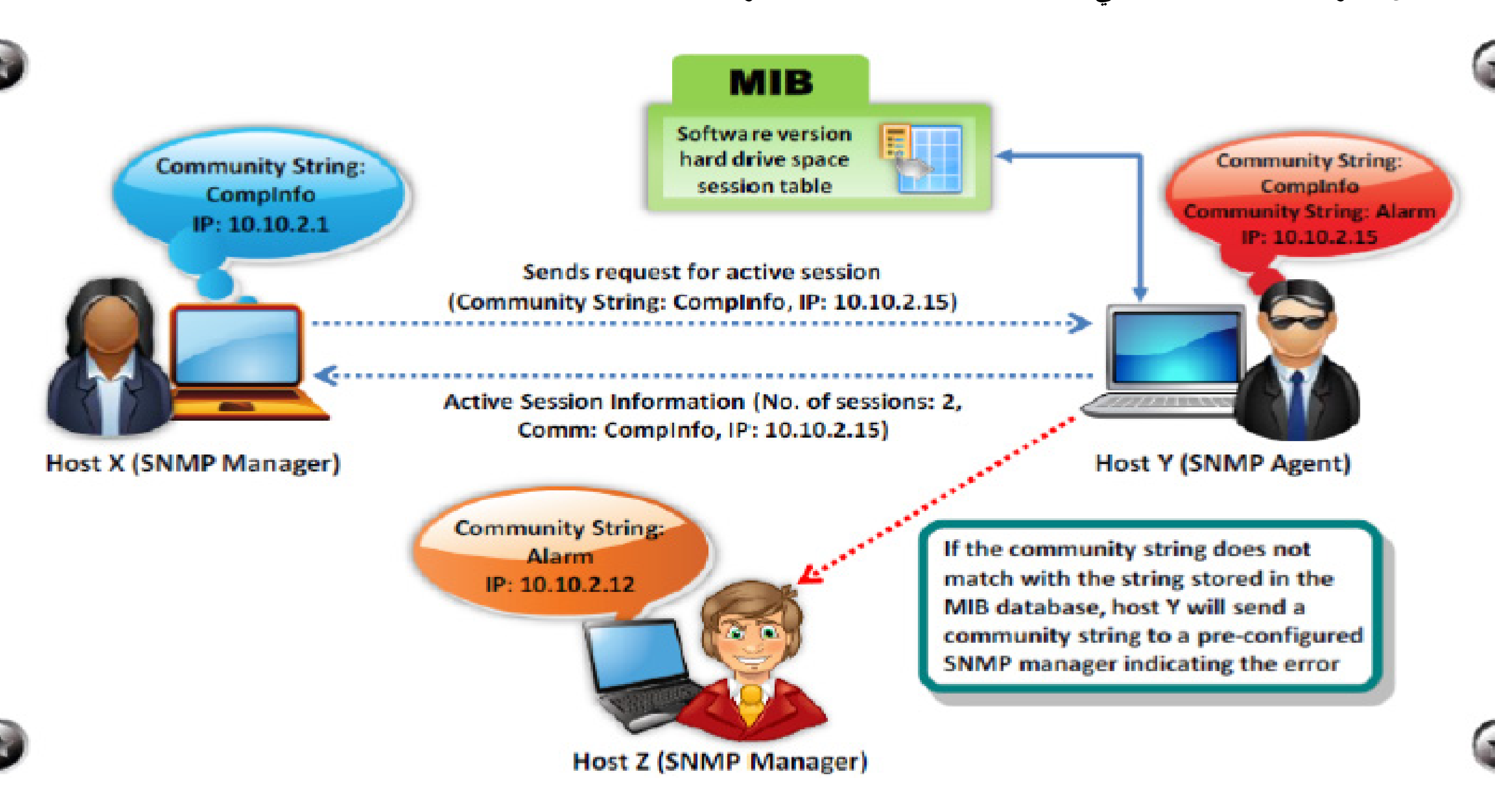
- **Read community string (كلمات المرور للقراءة فقط)**

اعداد الأجهزة (**devices**) والأنظمة يمكن رؤيتها بواسطة هذا النوع من كلمات المرور. كلمات المرور هذه تكون عامه (**public**)أي متاح للجميع.

- **Read/Write community string (كلمات المرور للقراءة والكتابة)**

مكنك تغير او إضافة اعداد الأجهزة (**devices**) أو الأنظمة بواسطة هذا النوع من كلمات المرور. كلمات المرور هذه تكون خاصه (**private**) أي متاح للجميع.
عندما يترك الاعداد الافتراضي لكلمات المرور (**Community String**)، بالإضافة إلى ذلك، **SNMP** لديه نقطة ضعف في نظام التوثيق: **الخاص private**(**rw**) **والعام public** (**r**). حيث يتم تمرير صيغ الاتصال هذه بطريقه غير مشفرة على الشبكة وغالبا ما تترك في حالاتها الافتراضية، الخاصة والعامة. والتي تتيح للمهاجمين باغتنام هذه الفرصة، والعثور على ثغرات في ذلك. بعد ذلك، يمكن المهاجم ان يستخدم كلمات السر الافتراضية هذه لتغيير أو عرض تكوين الجهاز أو النظام. المهاجمين يقوموا بتعداد **SNMP** لاستخراج المعلومات حول موارد الشبكة مثل المضيفين، والراوتر، والأجهزة، والمشاركات، وغيرها، وشبكة المعلومات مثل جداول **ARP**، جداول التوجيه (**routing table**)، معلومات الجهاز محددة، وإحصاءات حركة المرور.

تشمل الأدوات المستخدمة عادة في تعداد SNMP الـ SNMPUtil والـ IP Network Browser.



MANAGEMENT INFORMATION BASE (MIB)

MIB هي قاعدة بيانات افتراضية تحتوي على الوصف الرسمي لكافة كائنات/أجهزة شبكة الاتصال التي يمكن إدارتها باستخدام **SNMP**.
MIB هي عباره عن جمع لمعلومات التنظيم(**hierarchically organized information**) . فإنه يوفر التمثيل القياسي لمعلومات سيرفر **SNMP** (**SNMP Agent**) والتخزين. يتم التعرف على عناصر **MIB** باستخدام معرف الكائنات(**object identifiers**) .
معرف الكائن (**Object ID**) هو اسم رقمي يعطي للكائن، ويبدأ من جذر **MIB tree**. معرف الكائن هو رقم فريد يعرف الكائن الموجود في التسلسل الهرمي لل**MIB**.
<u>**تتضمن كائنات إدارة MIB (MIB-managed object)**</u> الكائنات العددية (**Scalar object**) التي تحدد كائن واحد وكائنات الجداول (**Tabular object**) التي تحدد مجموعة من مثيلات الكائن ذات الصلة. تشمل معرفات الكائن نوع الكائن مثل العداد(***counter***)، سلسلة(***string***)، أو العنوان(***address***)، مستوى الوصول (***access level***) مثل القراءة أو القراءة / الكتابة، حجم القيود(***size restrictions***) ، ومعلومات النطاق. يستخدم **MIB** بمثابة كتاب الشفرة من قبل مدير **SNMP** (**SNMP manager**) لتحويل أرقام **OID** إلى عرض قابل للقراءة.
محتويات **MIB** يمكن الوصول إليها وعرضها باستخدام مستعرض الويب إما عن طريق إدخال عنوان **IP** و**Lseries.mib** أو عن طريق إدخال اسم مكتبة ***DNS*** و**Lseries.mib**. على سبيل المثال،**http://IP.Address/Lseries.mib** أو **http://library_name/Lseries.mib**.
<u>**يوفر Microsoft قائمة MIBs التي تم تثبيتها مع خدمة SNMP في مجموعة موارد الويندوز. الرئيسية منها كالاتي:**</u>

- DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts

يقوم برصد حركة المرور بين سيرفر DHCP والمضيف عن بعد.

- HOSTMIB.MIB: Monitors and manages host resources

يقوم برصد وإدارة موارد المضيفين.

- LNMIB2.MIB: Contains object types for workstation and server services

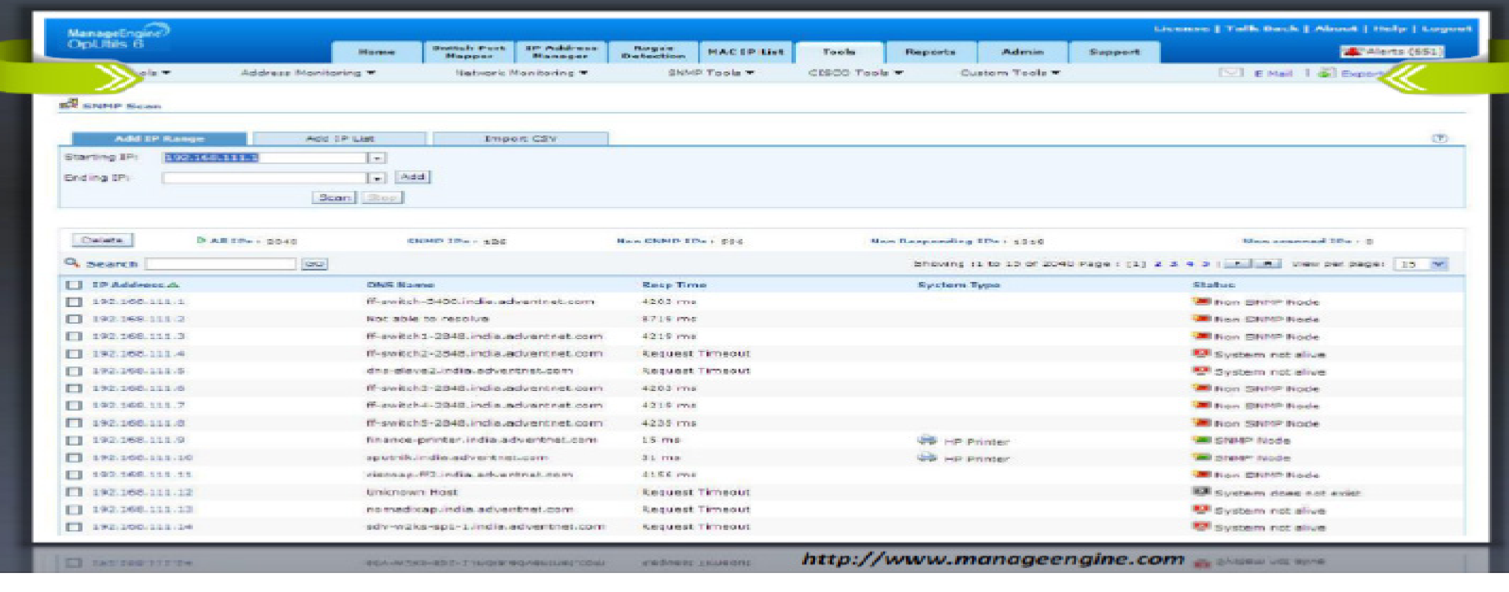
يحتوي على أنواع الكائنات.

- WINS.MIB: For Windows Internet Name Service

من اجل خادم WINS.

SNMP ENUMERATION TOOL: OPUTILS

المصدر: http://www.manageengine.com
OpUtils هو عبارة عن مجموعة من الأدوات التي تستخدم من قبل مهندسي الشبكة والتي يمكنها رصد وتشخيص واستكشاف موارد **IT** تكنولوجيا المعلومات. يمكنك رصد مدى توافر والأنشطة الأخرى للأجهزة الهامة، الكشف عن الوصول الغير مصرح به إلى شبكة الاتصال، وإدارة عناوين **IP**. أنها تسمح لك لإنشاء أدوات **SNMP** مخصصو والتي تمكنك مراقبة عقد **MIB** من خلالها.



SNMP ENUMERATION TOOL: SolarWind' s IP Network Browser

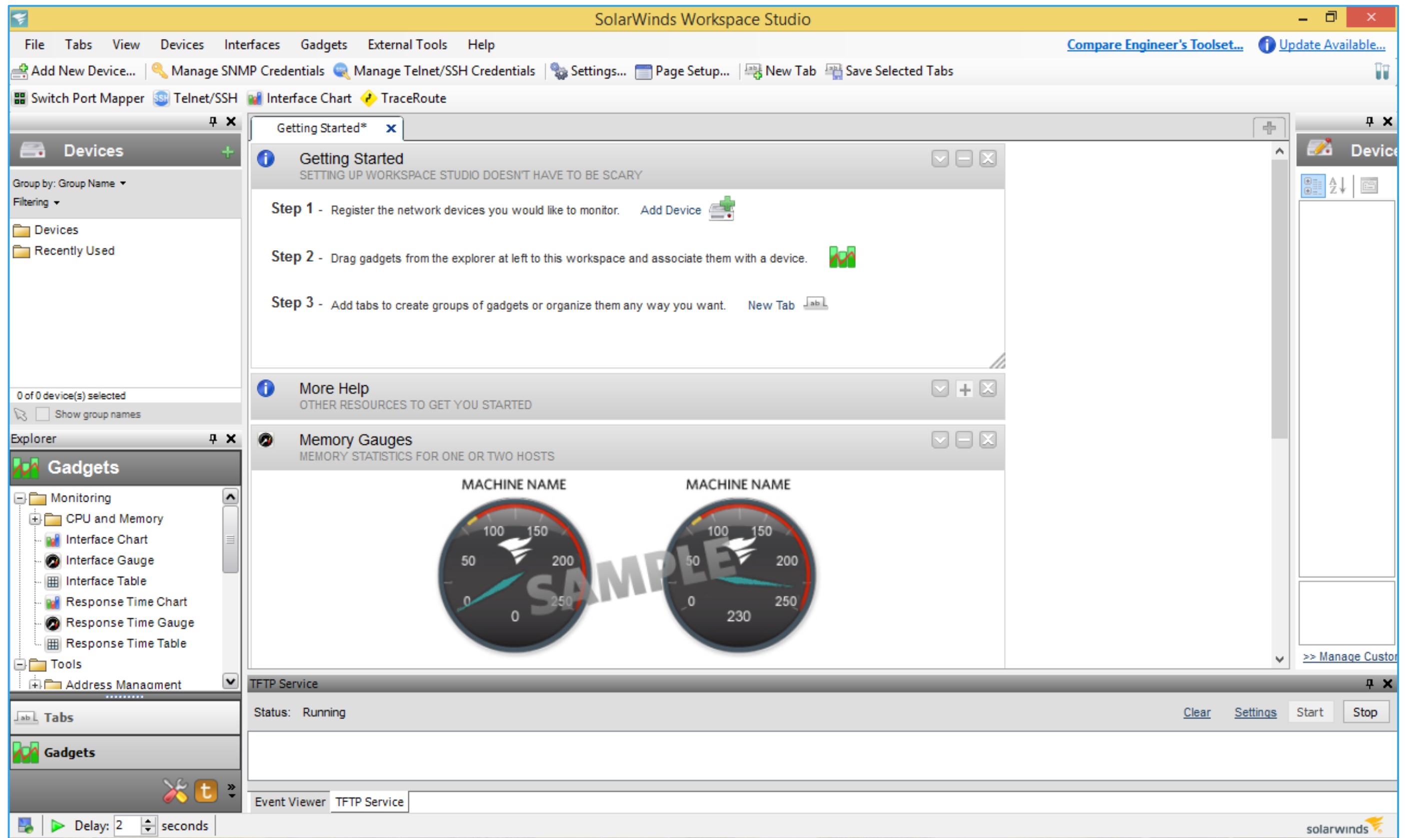
المصدر: http://www.solarwinds.com

SolarWind's IP Network Browser هو تطبيق لاكتشاف الشبكة. حيث يقوم بجمع المعلومات عن طريق **ICMP** و **SNMP** محليا أو على شبكة الاتصال البعيدة. يقوم بفحص **IP** واحد أو نطاق من عناوين **IP** أو الشبكة الفرعية، ثم يقوم بعرض أجهزة الشبكة التي تم اكتشافها في الوقت الحقيقي، مما يوفر لك الوصول الفوري إلى المعلومات المفصلة حول الأجهزة الموجودة على الشبكة. حيث يسهل على المهاجمين اكتشاف المعلومات حول الشبكة الهدف بعد تنفيذ عملية الفحص للشبكة الفرعية (**subnet**) بأكملها.

باستخدام **IP Network Browser**، فانه يمكن للمهاجم جمع المعلومات من نظام ويندوز تم اعداده بطريقه سيئة. وتشمل المعلومات التي يمكن جمعها اسم الملقم، إصدار نظام التشغيل، معلومات **SNMP** الاتصال ومعلومات الموقع، وقائمة الخدمات وواجهات شبكة الاتصال، قائمة بجميع حسابات المستخدمين، تاريخ آلة، وما الى ذلك.

على سبيل المثال، على جهاز التوجيه سيسكو(**Cisco router**) ، فأن **Solar Winds IP Network Browser** سوف يقوم بتحديد إصدار نظام التشغيل الحالي وإصداره، وكذلك تحديد أي من البطاقات التي تم تثبيتها البطاقات وفي أي فتحه(slots)، ووضع كل منفذ، وجدول **ARP**. عندما يكتشف **IP Network Browser** ملقم الويندوز، فإنه يعود بالمعلومات بما في ذلك وضع الواجهة (**interface**)، واستخدام **bandwidth**، والخدمات التي تعمل، وحتى تفاصيل البرامج التي تم تركيبها وتشغيلها.

1- نقوم بتثبيت التطبيق عن طريق اتباع **wizard** الخاص بعملية التثبيت، ثم تشغيله من خلال النقر فوق الأيقونة المعبرة عن التطبيق وهي **workspace studio** والتي تؤدى الى ظهور الشاشة التالية:



2- في شريط الادوات العلوي نختار **External Tools** والتي ينسدل منها قائمة أخرى نختار منها **Classic tools** ثم **Network Discovery** ثم **IP Network Browser**.

3- بعد النقر فوق ما سبق ذكره يؤدى الى ظهور الشاشة التالية:

IP Network Browser

File Edit Help

New Restart Export Print Copy Copy Stop Zoom Ping Telnet Trace Config Surf Settings Help

IP Network Browser

Scan a Single Device

Hostname or IP Address

Scan Device

Scan a Subnet

Subnet Address

Subnet Mask 255.255.255.0

Scan Subnet

Scan an IP Address Range

Begining IP Address

Ending IP Address

Scan Address Range

Engineer's Toolset v10 - Evaluation

4- نقوم بإدخال عنوان **IP** الخاص بالجهاز في المربع المقابل **Hostname or IP Address** ثم ننقر على **Scan device** والتي تقوم بعملي الفحص ثم بعد الانتهاء يعطيك ناتج الفحص في شاشه أخرى.

SNMP ENUMERATION TOOLS

بالإضافة إلى **OpUtils** و**SolarWind's IP Network Browser**، يتم سرد عدد قليل من أكثر أدوات **SNMP** على النحو التالي:

Getif available at http://www.wtcs.org
OiDViEW SNMP MIB Browser available at http://www.oidview.com
iReasoning MIB Browser available at http://tl1.ireasoning.com
SNScan available at http://www.mcafee.com
SNMP Scanner available at http://www.secure-bytes.com
SoftPerfect Network Scanner available at http://www.softperfect.com
SNMP Informant available at http://www.snmp-informant.com
Net-SNMP available at http://net-snmp.sourceforge.net
Nsauditor Network Security Auditor available at http://www.nsauditor.com
Spiceworks available at http://www.spiceworks.com

SNMP ENUMERATION TOOLS WITH KALI

1- الأداة snmpwalk

Snmpwalkهو تطبيق **SNMP** الذى يستخدم طلبات **SNMP GETNEXT** للاستعلام عن معلومات عن كيان شبكة الهدف. الان يمكنك جمع بعض المعلومات عن نظام تشغيل ويندوز الذي يعمل لدية الخدمة **SNMP** باستخدام الأمر التالي:

```
root@bt:~#snmpwalk©-c©public©-v1©<ip address>©1
```

والتي يمكنها الاستعلام عن مستخدمي الويندوز والخدمات التي تعمل مثال كالاتى:

```
root@bt:~#snmpwalk©-c©public©-v1©192.168.9.203©1©|©grep©hrSWRunName©|©cut -d" " -f4
```

يمكن الاستعلام عن المنافذ المفتوحة كالاتى:

```
root@bt:~#snmpwalk©-c©public©-v1©192.168.9.203©1©|©grep©tcpConnState©|©cut -d" " -f4
```

يمكنك الاستعلام عن التطبيقات المثبتة كالاتى:

```
root@bt:~#snmpwalk©-c©public©-v1©192.168.9.203©1©|©grep©hrSWInstalledName
```

Snmpcheck -2

اداه أخرى للحصول على معلومات عبر بروتوكولات **SNMP** هو **snmpcheck.**

```
#snmpcheck©-t©192.168.10.200
```

Braa -3

braa هي أداة لصنع استعلامات **SNMP**. أنها قادرة على الاستعلام لمئات أو آلاف المضيفين في وقت واحد، في حين انها تظهر كأنها عملية واحده تماما. أنها لا تحتاج إلى أي من مكتبات **SNMP**، كما أنها مزودة بمحرك **SNMP**. ومع ذلك، فإنه من الجيد أن يكون لديك مجموعة كاملة من حزم **SNMP** بما في ذلك **snmptranslate** المثبتة في مكان ما، وذلك لأسباب السرعة، لا يوجد أي محلل **ASN.1** في **braa**، ويحتاج **SNMP OIDs** ان تحدد عدديا.

```
#braa©10.253.101.1-10.253.101.50:.1.3.6.1.2.1.1.6.0
```

cisco-auditing-tool -4

Cisco Auditing Tool- هو نص بيرل الذي يفحص موجهات سيسكو لإيجاد نقاط الضعف الشائعة. يفحص كلمات السر الافتراضية، وأسماء التي يسهل تخمينها، وتاريخ علة نظام التشغيل. ويشمل الدعم للملحقات والفحص للمضيفين متعددين.

الصيغة العامة لها كالاتى:

```
#CAT©[options]
```

OPTIONS

- -h hostname (for scanning single hosts)
- -f hostfile (for scanning multiple hosts)
- -p port # (default port is 23)
- -w wordlist (wordlist for community name guessing)
- -a passlist (wordlist for password guessing)
- -i [ioshist] (Check for IOS History bug)
- -l logfile (file to log to, default screen)
- -q quiet mode (no screen output)

مثال على ذلك كالاتى:

```
#CAT©-h©192.168.1.100©-w©wordlist©-a©passwords©-i
```

onesixtyone -5

Onesixtyone يستفيد من حقيقة أن SNMP هو بروتوكول بدون اتصال (**connectionless protocol**) ويرسل جميع طلبات **SNMP** بأسرع ما يمكن. ثم ينتظر الفاحص الردود للعودة وتسجلهم، فهو يشبه **Nmap ping sweeps**. افتراضيا ينتظر **onesixtyone** لمدة 10 ميلي ثانية بين إرسال الحزم، والتي تكافئ 100MBs من تحولات الشبكات(**switched network**) . يمكن للمستخدم ضبط هذه القيمة عن طريق خيار سطر الأوامر(-w). إذا تم تعيينها إلى 0، فان الفاحص سوف يقوم بإرسال الحزم بالسرعة التي سوف يستقبلها الكيرنل، مما قد يؤدي إلى اسقاط او فقدان الحزمة.

الصيغة العامة كالاتى:

```
#onesixtyone©[options]©<host>©<community>
```

Options

-c <communityfile> file with community names to try
-i <inputfile> file with target hosts
-o <outputfile> output log
-d debug mode, use twice for more information
-w <n> wait n milliseconds (1/1000 of a second) between sending packets (default 10)
-q quiet mode، do not print log to stdout، use with -l

مثال كالاتى:

#onesixtyone©192.168.1.1

UNIX/LINUX ENUMERATION 4.4

يصف هذا القسم الأوامر يونيكس/لينكس التي يمكن استخدامها للتعداد وأدوات تعداد لينكس. الأوامر المستخدمة لتعداد موارد شبكة يونكس او لينكس هي كما يلي: **showmount**، **finger**، **rpcinfo** (**RPC**)، و**rpcclient**.

finger
- Enumerates the user and the host
- Enables you to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail

```
[root$] finger -l @target.hackme.com
```

rpcinfo (RPC)
- Helps to enumerate Remote Procedure Call protocol
- RPC protocol allows applications to communicate over the network

```
[root] rpcinfo -p 19x.16x.xxx.xx
```



- Using rpcclient we can enumerate user names on Linux and OS X

```
[root $] rpcclient $> netshareenum
```

showmount
- Finds the shared directories on the machine

```
[root $] showmount -e 19x.16x. xxx.xx
```

FINGER

يتم استخدام الأمر **finger** لتعداد المستخدمين على الجهاز البعيد. تمكنك أيضا من عرض مجلد الـ **Home**الخاص بالمستخدمين، وقت تسجيل الدخول(**login time**) ، أوقات الخمول(**idle time**) ، موقع المكتب، وآخر مرة تلقى أو قراءة البريد.

الصيغة العاملة:

#finger [-b] [-f] [-h] [-i] [-l] [-m] [-p] [-q] [-s] [-w] [username]

الخيارات[Options]:

[-b]: يمنع طباعة المجلد الرئيسي للمستخدم (**home directory**) والشل المستخدم في ناتج الامر والذى يكون على شكل نسخة مطبوعة طويلة.

[-f]: يمنع طباعة الرأس (**head**) والتي يتم طباعتها عادة في شكل النسخة مطبوعة الغير طويلة لناتج الامر.

[-h]: يمنع طباعة الملف {**.project**} في ناتج الامر والذى يكون على شكل نسخة مطبوعة طويلة.

[-i]: يجبره ناتج الامر **finger** في الظهور على صيغة [**idle**] ، والتي تشبه الشكل القصير(**short output**) إلا أنه يتم طباعة فقط اسم تسجيل الدخول، الترمنال، وقت تسجيل الدخول، ووقت الخمول[**idle**] .

[-l]: يجبره ناتج الامر **finger** في الظهور على صيغة الشكل الطويل (**long output format**).
[-m]: يطابق المعاملات فقط على اسم المستخدم (**Matches arguments only on the user's name**).
[-p]: يمنع طباعة الملف {**.plan**} في ناتج الامر والذى يكون على شكل نسخة مطبوعة طويلة.
[-q]: يجبره على الظهور على هيئة تنسيق سريع (**quick output**) ، الذي يشبه الشكل القصير(**short output**) إلا أنه يتك طباعة فقط اسم تسجيل الدخول، الترمنال، ووقت الدخول.
[-s]: يجبره على الظهور على هيئة تنسيق قصير(**short output**) .
[-w]: يمنع طباعة الاسم بالكامل في التنسيق القصير.
على سبيل المثال، إذا تم تنفيذ الأمر [**root$finger©-1©@target.hackme.com**]، فأنه يمكنك الحصول على قائمة المستخدمين على المضيف الهدف.

Rpcinfo (RPC)

Rpcinfo (RPC) يساعدك على تعداد بروتوكول استدعاء الإجراء البعيد[**Remote Procedure Call protocol**] . وهذا بدوره يسمح للتطبيقات على التواصل عبر الشبكة.

الصيغة العامة:

```
rpcinfo [-m | -s ] [ host ]
rpcinfo -p [ host ]
rpcinfo -T transport host prognum [ versnum ]
rpcinfo -l [ -T transport ] host prognum versnum
rpcinfo [ -n portnum ] -u host prognum [ versnum ]
rpcinfo [ -n portnum ] -t host prognum [ versnum ]
rpcinfo -a serv_address -T transport prognum [ versnum ]
rpcinfo -b [ -T transport ] prognum versnum
rpcinfo -d [ -T transport ] prognum versnum
```

الخيارات (Options):

[-m]: يعرض جدول الإحصاءات [**Static table**] إحصائيات لعمليات **rpcbind** على مضيف معين. ويبين الجدول إحصاءات لكل إصدار من **rpcbind** (الإصدارات 2 و3 و4)، ويعطى عدد المرات التي تم طلبها لكل إجراء والخدمات بنجاح، عدد ونوع الطلبات الدعوة عن بعد [**remote call request**] التي تم إجراؤها، والمعلومات حول عمليات بحث عنوان **RPC** التي تم التعامل معها. وهذا مفيد لرصد أنشطة **RPC** على المضيف.
[-s]: يعرض قائمة مختصرة لجميع برامج **RPC** المسجلة على المضيف. إذا لم يتم تحديد المضيف، فإنه يفترض المضيف المحلي.
[-p]: يتحقق من خدمة **rpcbind** على المضيف باستخدام الإصدار 2 من بروتوكول **rpcbind**، ثم يعرض قائمة من كافة برامج **RPC** المسجلة. إذا لم يتم تحديد المضيف، فإنه يفترض المضيف المحلي. لاحظ أن الإصدار 2 من بروتوكول **rpcbind** كان يعرف سابقا باسم بروتوكول **portmapper**.
[-t]: يجعل **RPC Call** للإجراء 0 ل **prognum** على المضيف المحدد الذى يستخدم **TCP**، ويعطى تقرير ما إذا تلقى أي رد. هذا التعبير يتم اهماله عند استخدام [-T]كما هو مبين في الجملة الثالثة.
[-l]: يعرض قائمة الإدخالات مع **prognum** و**versnum** على المضيف المحدد. يتم إرجاع الإدخالات لجميع الـ **transport** الموجودة في عائلة البروتوكول نفسه والتي تستعمل في اتصالات **rpcbind** البعيد.
[-b]: يجعل **RPC broadcast** للإجراء 0 ل **prognum** و**versnum** المحددة, ثم يعطى تقرير عن كل المضيفين الذين استجابوا. إذا تم تحديد **transport**، **فإن broadcast** يرسل طلباته فقط على **transport** المحدد. إذا لم يتم تحديد **broadcast** بأي **transport**، فتتم طباعة رسالة خطأ. استخدام **broadcast** (التعبير **b–**) ينبغي أن يكون محدود بسبب احتمال التأثير السلبي على الأنظمة الأخرى.
[-d]: يحذف التسجيلات الخاصة بالسيرفس **RPC** ل **prognum** و**versnum** المحددة. إذا تم تحديد **transport**، فأن إلغاء الخدمة يكون فقط على ذلك **transport**، وإلا فان سوف يتم إلغاء الخدمة على جميع **transport** التي تم التسجيل عليها. هذا الخيار لا يمكن أن يمارس إلا من قبل المستخدم الجذري.

[-u]: يجعل **RPC Call** للإجراء 0 ل **prognum** على المضيف المحدد الذى يستخدم **UDP**، ويعطى تقرير ما إذا تلقى أي رد. هذا التعبير يتم اهماله عند استخدام **[-T]**كما هو مبين في الجملة الثالثة.

[-a serv_address]: يستخدم **serv_address** كعنوان (**universal**) للخدمة على الـ **transport** لعمل**ping** للإجراء 0 ل **prognum** المحدد والتقرير في حالة استلام الرد او من عدمه. الخيار **T-**مطلوب مع الخيار**a-** .

إذا لم يتم تحديد **versnum**، فان **rpcinfo**سوف يقوم بعمل **ping** لجميع أرقام الإصدارات المتاحة لهذا العدد من البرنامج. ويتجنب هذا الخيار دعوة **rpcbind** البعيد للبحث عن عنوان الخدمة. يتم تحديد **Serv_address**في تنسيق العنوان العالمي لـ **transport**المعطى.

[-n Portnum]: يستخدم المعامل **Portnum** على أنه رقم المنفذ للخيارات **t-** و**u-** بدلا من رقم المنفذ الذي قدم من قبل **portmap**.

باستخدام الخيار n– فانه يتجنب دعوة إلى **portmap** من بعيد لمعرفة عنوان الخدمة. هذا التعبير يتم اهماله عند استخدام**[-a]**.

[-T]: تعين الـ **Transport**حيث الخدمة مطلوبة. إذا لم يتم تحديد هذا الخيار فان **rpcinfo** يستخدم الـ**Transport** المحدد في المتغير البيئي (**environment variable**) **NETPATH**، او إذا لم يتم تعينه او تم تعينه الى **NULL** فان يستخدم **transport** الموجود في قاعدة بيانات اعداد الشبكة (**netconfig database**). هذا الخيار خيار عامي، ويمكن استخدامه للاقتران مع الخيارات أخرى كما هو موضح 'في الملخص'.

[Host]: تحدد المضيف التي يتم جمع معلومات **rpc** المطلوبة منها.

على سبيل المثال، إذا تم تنفيذ الأمر [**root$rpcinfo©-p19x.16x.xxx.xx**]، فأنه يمكنك الحصول على معلومات rpc عن المضيف الهدف الذي تتصل به حاليا.

RPCCLIENT

Rpcclient يستخدم في تعداد أسماء المستخدمين في لينكس، و**OS X**. وهى أيضا أداة لتنفيذ مهام العميل MS-RPC. ويعتبر أداة من أدوات خادم **SAMBA**.

الصيغة العامة:

#rpcclient [-A authfile] [-c <command string>] [-d debuglevel] [-h] [-l logdir] [-N] [-s <smb config file>] [-U username [%password]] [-W workgroup] [-I destinationIP] {server}

الخيارات (Options):

[-c <command string>]: يعمل على تنفيذ الأوامر المفصولة بفاصلة منقوطة(;) على جهاز العميل.

[-I destinationIP]: عنوان IP هو عنوان الملقم للاتصال. وينبغي أن يحدد ذلك في المعيار "a.b.c.d".

[-p portnum]: هذا الرقم هو رقم منفذ **TCP** الذي سوف يتم استخدامه عند إجراء اتصالات إلى الملقم. المعيار الافتراضي لرقم منفذ **TCP** لملقم **SMB / CIFS** هو 139.

[-d debuglevel]: **debuglevel** هو عدد صحيح من 0 إلى 10. القيمة الافتراضية إذا لم يتم تحديد هذا المعامل فيصبح 0.

عند ارتفاع هذه القيمة، فانه سوف يتم تسجيل مزيد من التفاصيل في ملفات السجل (**log file**) عن أنشطة الخادم. على مستوى 0، سيتم تسجيل فقط الأخطاء الفادحة (**critical errors**) والتحذيرات الخطيرة(**serious warnings**) . المستوى 1 هو مستوى معقول – حيث أنه يولد كمية صغيرة من المعلومات حول العمليات التي يقوم بها.

والمستويات أعلى من 1 تولد كميات كبيرة من بيانات السجل، ويجب استخدامه فقط عند التحقيق في مشكلة ما. صممت مستويات فوق 3 للاستخدام فقط من قبل المطورين وتوليد كميات ضخمة من بيانات السجل، ومعظمها غير خفي للغاية.

[-V]: يطبع رقم إصدار البرنامج.

[-s <smb config file>]: الملف المحدد يحتوي على تفاصيل الاعداد المطلوبة من قبل الملقم. وتشمل المعلومات في هذا الملف معلومات الملقم المحددة مثل ما هو ملف **printcap** المستخدم، فضلا عن أوصاف لكافة الخدمات التي يوفرها الملقم لتوفير. انظر الى الملف **smb.conf** لمزيد من المعلومات. يتم تحديد اسم الملف الاعداد الافتراضي في وقت ترجمة الخادم من قبل الكيرنل(**compile**).

[-l logdirectory]: اسم المجلد الذى يحتوى على ملفات السجل/التصحيح(**log/debug**) . الامتداد ".progname" التي سوف يتم إلحاقها (على سبيل المثال log.smbclient، log.smbd، الخ ..). لن تتم إزالة ملفات السجل أبدا من قبل العميل.

[-N]: إذا تم تحديده، فان هذا المعامل يمنع المطالبة بكلمة المرور العادية من العميل للمستخدم. وهذا مفيد عند الوصول إلى الخدمة التي لا تتطلب كلمة مرور.

[-A authfile]: يسمح لك هذا الخيار لتحديد ملف يمكن من خلالها قراءة اسم المستخدم وكلمة المرور المستخدمة في الاتصال. تنسيق هذا الملف كالاتى:

```
username = &lt;value>
password = &lt;value>
domain   = &lt;value>
```

[-U username [%password]]: يستخدم لوضع اسم المستخدم أو اسم المستخدم وكلمة المرور **SMB**.

[-W domain]: يستخدم لتعيين دومين **SMB** من اسم المستخدم. هذا يتجاوز الدومين الافتراضي والذي هو الدومين المعرف في ملف الاعداد **smb.conf**. إذا كان الدومين المحدد هو نفس اسم خوادم **NETBIOS**، فإنه يتسبب العميل لتسجيل الدخول باستخدام خوادم **SAM** المحلية (في مقابل **SAM** الدومين).

[-h]: يقوم بطابعة ملخص للخيارات المتاحة لهذا الامر (ملفات المساعدة).

SHOWMOUNT

Showmount يحدد ويسرد المجلدات المشتركة المتوفرة على النظام. يتم سرد العملاء التي يتم تحميلهم (**mounted**)عن بعد على نظام الملفات من المضيف باستخدام الامر **showmount**. **Mountd** هو خادم **RPC** والذى يقوم بالردود على الوصول إلى معلومات نظام الملفات NFS وطلبات التحميل على نظام الملفات (**filesystem mount request**). خادم **mountd** على المضيف يحافظ على المعلومات التي يتم الحصول عليها. الملف **/etc/rmtab** يحفظ المعلومات الناتجة من **crashing**. القيمة الافتراضية للمضيف هو القيمة التي تم إرجاعها من قبل المضيف (1). يستخدم هذا الأمر من قبل أي جهاز على الشبكة لمعرفة الأجهزة المستفيدة من خدمة NFS.

الصيغة العامة للخادم **mountd** كالاتى:

#usr/lib/nfs/mountd [-v] [-r]

الصيغة العامة للخادم **showmount** كالاتى:

#/usr/sbin/showmount [-ade] [hostname]

الخيارات المتاحة مع الامر showmount كالاتى:

1-[showmount –a]:

يستخدم هذا الأمر على خادم NFS لمعرفة الأجهزة التي تصل إلى المجلدات المشاركة.

2-[showmount –e]:

يستخدم هذا الأمر لعرض قائمة المجلدات المشاركة من خادم **NFS**بذكر اسم الخادم بعد الأمر مثال على ذلك كالاتى:

#showmount©-e©server1.example.com

```
Export list for server1.example.com:
/mnt   192.168.100.0/24
/home  192.168.122.0/24
```

3-[showmount –d]:

يستخدم هذا الأمر على خادم NFS لعرض قائمة المجلدات المشاركة فقط أي التي أنشاء لها نقطة ضم (**mounted**)لدى العملاء **client**

#showmount©-d©server1.example.com

```
Directories on server1.example.com:
/home
/mnt
```

ملحوظه: إذا لم يعمل هذا الأمر جيدا، فاعلم انه يكون نتيجة حظر الاتصال من قبل جدار حماية.

LINUX ENUMERATION TOOL: ENUM4LINUX

المصدر: https://labs.portcullis.co.uk

Enum4linux هو الأداة التي تسمح لك بتعداد المعلومات من خادم السامباء، وكذلك أنظمة الويندوز.

المميزات:

- RID Cycling (When RestrictAnonymous is set to 1 on Windows 2000)
- User Listing (When RestrictAnonymous is set to 0 on Windows 2000) قائمة بالمستخدمين
- Listing of Group Membership Information معلومات عن قائمة المجموعات العضو

- Share Enumeration — تعداد المشاركة
- Detecting if host is in a Workgroup or a Domain — الكشف عن حالة المضيف هل هو في مجموعة عمل أو دومين
- Identifying the remote Operating System — تحديد نظام التشغيل عن بعد
- Password Policy Retrieval (using polenum) — سياسة استرجاع كلمات السر

```
sh-3.2$ enum4linux.pl -r 192.168.2.55
Starting enum4linux v0.8.2 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:14:35 20(

----- Target information -----
Target ........... 192.168.2.55
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- Enumerating Workgroup/Domain on 192.168.2.55 ------
[+] Got domain/workgroup name: WORKGROUP

----- Getting domain SID for 192.168.2.55 -----
Domain Name: WORKGROUP
Domain Sid: S-0-0
[+] Host is part of a workgroup (not a domain)

----- Session Check on 192.168.2.55 -----
[+] Server 192.168.2.55 allows sessions using username '', password ''

----- Users on 192.168.2.55 via RID cycling (RIDS: 500-550,1000-1050) -----
[I] Assuming that user "administrator" exists
[+] Got SID: S-1-5-21-1801674531-1482476501-725345543 using username '', password ''
S-1-5-21-1801674531-1482476501-725345543-500 W2KSQL\Administrator (Local User)
S-1-5-21-1801674531-1482476501-725345543-501 W2KSQL\Guest (Local User)
S-1-5-21-1801674531-1482476501-725345543-513 W2KSQL\None (Domain Group)
S-1-5-21-1801674531-1482476501-725345543-1000 W2KSQL\TsInternetUser (Local User)
S-1-5-21-1801674531-1482476501-725345543-1001 W2KSQL\IUSR_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1002 W2KSQL\IWAM_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1004 W2KSQL\mark (Local User)
S-1-5-21-1801674531-1482476501-725345543-1005 W2KSQL\blah (Local User)
S-1-5-21-1801674531-1482476501-725345543-1006 W2KSQL\basic (Local User)

enum4linux complete on Wed Apr  2 14:14:40 2008
```

LDAP ENUMERATION 4.5

لتمكين الاتصال وإدارة نقل البيانات بين موارد الشبكة، وتشغيل البروتوكولات المختلفة. كل هذه البروتوكولات تحمل معلومات قيمة عن موارد الشبكة جنبا إلى جنب مع البيانات التي يتم نقلها. إذا كان أي مستخدم خارجي قادر على تعداد تلك المعلومات عن طريق التلاعب في البروتوكولات، فانه يمكن أن يقتحم الشبكة ويمكن إساءة استخدام موارد الشبكة. **LDAP** هو واحد مثل هذه البروتوكولات والتي يهدف للوصول إلى قوائم الدليل. هذا القسم سوف يركز على تعداد **LDAP** والأدوات المستخدمة في عملية التعداد.

يتم استخدام البروتوكول (**LDAP**) (***Lightweight Directory Access Protocol***) للوصول إلى قوائم الدليل ضمن الـ **Active Directory** أو من خدمات الدليل الأخرى(**other directory services**) . يتم تجميع الدليل في شكل هرمي أو منطقي، مثل مستويات الإدارة والموظفين في الشركة. انها مناسبة لترتبط مع خادم الاسماء (**DNS**) للسماح لعمليات البحث السريع والقرار السريع للاستفسار. وعادة ما يعمل على المنفذ 389 والبروتوكولات الأخرى المماثلة. يمكنك الاستعلام عن خدمة **LDAP** بطريقه مجهولة. سيقوم الاستعلام بالكشف عن معلومات حساسة مثل أسماء المستخدمين وعناوين وتفاصيل الإدارات، أسماء الملقمات وغيرها، والتي يمكن استخدامها من قبل المهاجم لإطلاق الهجوم.

LDAP ENUMERATION TOOL: SOFTERRA LDAP ADMINISTRATOR

المصدر: http://www.ldapadministrator.com

Softerra LDAP Administrator هو أداة لإدارة **LDAP** التي تسمح لك بالعمل مع خوادم **LDAP** مثل **Active Directory**، **Novell Directory Services** ، **Netscape/iPlanet** ، وهكذا. فهو يولد تقارير الدليل القابلة للتخصيص مع المعلومات اللازمة لرصد وتدقيق فاعليته.

المميزات:

- توفر إمكانية البحث في الدليل، عمليات التحديث بالجملة(**bulk update operation**) ، إدارة عضوية المجموعة، الخ
- يدعم **LDAP-SQL**، والذي يسمح لك بإدارة إدخالات **LDAP** باستخدام صيغه مثل **SQL**.

HTML View

LDAP Administrator

http://www.ldapadministrator.com

LDAP ENUMERATION TOOLS

هناك العديد من الأدوات لتعداد **LDAP** التي يمكن استخدامها للوصول إلى قوائم الدليل ضمن **Active Directory** أو من خدمات الدليل الأخرى. يمكن استخدام هذه الأدوات من قبل المهاجمين لتعداد المعلومات مثل أسماء المستخدم الصالحة والعناوين وتفاصيل الإدارات، وما إلى ذلك من خوادم **LDAP** المختلفة.

يتم سرد عدد قليل من أدوات تعداد LDAP على النحو التالي:

JXplorer available at http://www.jxplorer.org
LDAP Admin Tool available at http://www.ldapsoft.com
LDAP Account Manager available at http://www.ldap-account-manager.org
LEX - The LDAP Explorer available at http://www.ldapexplorer.com
LDAP Admin available at http://www.ldapadmin.org
Active Directory Explorer available at http://technet.microsoft.com
LDAP Administration Tool available at http://sourceforge.net
LDAP Search available at http://securityxploded.com
Active Directory Domain Services Management Pack available at http://www.microsoft.com
LDAP Browser/Editor available at http://www.novell.com

NTP ENUMERATION 4.6

في كثير من الأحيان، يتم التغاضي عنه خادم **NTP** من الناحية الأمنية. ولكن، إذا كان الاستعلام بشكل صحيح، فإنه يمكن أيضا أن يوفر الكثير من المعلومات القيمة عن الشبكة الهدف بالنسبة للمهاجمين. وبالتالي، فمن الضروري اختبار ما هي المعلومات التي يمكن للمهاجم تعدادها حول الشبكة من خلال تعداد **NTP**.

يصف هذا القسم ما هو **NTP**، ما هي المعلومات التي يمكن استخراجها من خلال عملية تعداد **NTP**، والأوامر المستخدمة في ذلك.

قبل البدء مع تعداد**NTP** ، دعونا أولا مناقشة ما هو**NTP** . **NTP** هو اختصار لـ **Network Time Protocol**وهو بروتوكول شبكة مصمم لمزامنة الساعة في أنظمة الكمبيوتر المتصلة بالشبكة. **NTP** مهم عند استخدام خدمات الدليل(**Directory Services**) . يستخدم المنفذ **UDP 123** كوسيلة رئيسيه للاتصال . **NTP** يمكنه الحفاظ على الوقت في غضون 10 ميلي ثانية (1/100 ثانية) على شبكة الإنترنت العامة . فإنه يمكن تحقيق الدقة من 200 ميكرو ثانية أو أفضل في الشبكات المحلية تحت ظروف مثالية.

من خلال تعداد **NTP**، يمكنك جمع المعلومات مثل قوائم المضيفين (**List of hosts**) المتصلة بخادم **NTP**، عناوين IP، أسماء النظام، ونوع نظام التشغيل الذي يعمل على أنظمة العميل في الشبكة. كل هذه المعلومات يمكن تعدادها بواسطة الاستعلام عن خادم **NTP**. إذا كان ملقم **NTP** في **DMZ**، فإنه يمكن أيضا أن يكون من الممكن الحصول على عناوين **IP** الداخلية.

NTP ENUMERATION COMMANDS

تعداد **NTP** يمكن تنفيذها باستخدام أدوات سطر الأوامر **NTP** (**NTP suite command-line tool**). يستخدم تطبيقات **NTP** للاستعلام من خادم **NTP** للحصول على المعلومات المطلوبة من **NTP**. يشمل موجوعة أدوات سطر الأوامر الخاصة بالـ **NTP**كالاتى:

ntptrace
ntpdc
ntpq

هذه الأوامر سوف تساعدك على استخراج البيانات من بروتوكول **NTP** المستخدمة في الشبكة المستهدفة.

NTPTRACE

Ntptrace هو سكريبت من النوع بيرل لنظام التشغيل لينكس/يونكس الذي يستخدم برنامج الأداة المساعدة **ntpq** لمتابعة سلسلة من خوادم **NTP** من المضيف وذلك بالنظر الى الوراء الى مصدر الوقت الأساسي وذلك لتحديد المواكن الذى يقوم خادم **NTP** بتحديث وقته.

الصيغة العامة كالاتى:

#ntptrace [-vdn] [-r retries] [-t timeout] [servername/IPaddress]

امثله على ذلك كالاتى:

```
root@jana:~# ntptrace
localhost: stratum 3, offset 0.000000, synch distance 0.114775
41.231.7.85: timed out, nothing received
***Request timed out
root@jana:~#
```

NTPDC

هذا الأمر يساعدك على الاستعلام عن **NTP daemon** وهو **ntpd** عن وضعها الحالي وإمكانية التغير في حالتها.

الصيغة العامة كالاتى:

#ntpdc [-ilnps] [-c command] [hostname/IPaddress]

```
root@jana:~# ntpdc
ntpdc> ?
ntpdc commands:
addpeer        controlkey    fudge         keytype       quit          timeout
addrefclock    ctlstats      help          listpeers     readkeys      timerstats
addserver      debug         host          loopinfo      requestkey    traps
addtrap        delay         hostnames     memstats      reset         trustedkey
authinfo       delrestrict   ifreload      monlist       reslist       unconfig
broadcast      disable       ifstats       passwd        restrict      unrestrict
clkbug         dmpeers       iostats       peers         showpeer      untrustedkey
clockstat      enable        kerninfo      preset        sysinfo       version
clrtrap        exit          keyid         pstats        sysstats
ntpdc> monlist
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
ns2.atlax.com            123 192.168.1.106         22 4 4    1d0     42       1
a.ntp.ru.ac.za           123 192.168.1.106         21 4 4    1d0     44      12
ns3.atlax.com            123 192.168.1.106         20 4 4    1d0     46      17
ops2.neology.co.za       123 192.168.1.106         21 4 4    1d0     44      38
ntpdc>
```

NTPQ

هذا الأمر يساعدك على مراقبة عمليات **NTP daemon** وهو **ntpd** وتحديد الأداء.

الصيغة العامة كالاتى:

#ntpq [-inp] [-c command] [host/IPaddress]

```
root@jana:~# ntpq
ntpq> ?
ntpq commands:
:config         delay           mreadvar        readlist
addvars         exit            mrl             readvar
associations    help            mrv             rl
authenticate    host            ntpversion      rmvars
cl              hostnames       opeers          rv
clearvars       keyid           passociations   saveconfig
clocklist       keytype         passwd          showvars
clockvar        lassociations   peers           timeout
config-from-file lopeers        poll            version
cooked          lpassociations  pstatus         writelist
cv              lpeers          quit            writevar
debug           mreadlist       raw
ntpq> version
ntpq 4.2.6p5@1.2349-o Sat May 12 09:07:20 UTC 2012 (1)
ntpq> host
current host is localhost
ntpq> readlist
associd=0 status=0618 leap_none, sync_ntp, 1 event, no_sys_peer,
version="ntpd 4.2.6p5@1.2349-o Sat May 12 09:07:18 UTC 2012 (1)",
processor="i686", system="Linux/3.7-trunk-686-pae", leap=00, stratum=3,
precision=-19, rootdelay=311.410, rootdisp=384.484, refid=41.73.40.9,
reftime=d6ff7423.14a2df8f  Mon, Apr 21 2014 12:40:35.080,
clock=d6ff755c.f1dbf0e1  Mon, Apr 21 2014 12:45:48.944, peer=15856, tc=6,
mintc=3, offset=3.388, frequency=24.063, sys_jitter=11.021,
clk_jitter=30.244, clk_wander=0.915
ntpq>
```

SMPT ENUMERATION 4.7

حتى الآن، ناقشنا ما هو التعداد وتقنيات التعداد لاستخراج المعلومات التي تتعلق بموارد الشبكة. الآن حان الوقت لمناقشة أسلوب التعداد التي يمكن استخراج المعلومات ذات الصلة بالمستخدمين الموجودين على خادم **SMTP**، أي تعداد **SMTP**.

سيكون هذا القسم تعريفي في كيفية الحصول على قائمة المستخدمين الصالحة على الملقم **SMTP** والأدوات التي يمكن اختبار عملية إرسال البريد الإلكتروني من خلال خادم **SMTP**.

تعداد **SMTP** يسمح لك بتحديد المستخدمين على ملقم **SMTP**. ويتم إنجاز هذا من قبل ثلاث أوامر **built-in SMTP command** . هذه الأوامر كالاتى:

VRFY يتم استخدام هذا الأمر للتحقق من صحة المستخدمين.

EXPN هذا الأمر يخبرك بعنوان التسليم الفعلي للأسماء المستعارة (**alias name**) والقوائم البريدية

RCPT TO هو يحدد مستلمي الرسالة.

خوادم **SMTP** تستجيب بشكل مختلف للأوامر **VRFY**، **EXPN**، و**RCPT** من اجل اسم المستخدم الصالح (**valid user**) والغير صالح(**invalid user**) . وبالتالي، من خلال مراقبة استجابة الملقم **SMTP** لهذه الأوامر، يمكن للمرء بسهولة تحديد المستخدمين الصالح (**valid user**)على الملقم **SMTP**. يمكن للمهاجم أيضا التواصل مباشرة مع خادم **SMTP** من خلال الامر **telnet** على النحو التالي:

Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User
<Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP ENUMERATION TOOL: NETSCANTOOLS PRO

المصدر: http://www.netscantools.com

NetScanTools Pro's SMTP Email Generator tool يسمح لك باختبار عملية إرسال رسالة البريد الإلكتروني من خلال خادم **SMTP**. يمكنك استخراج جميع المعاملات الأكثر شيوعا من رأس البريد الإلكتروني بما في ذلك **confirm/urgent flags**. يمكنك تسجيل دخول جلسة البريد الإلكتروني إلى ملف السجل ثم تقوم بمشاهدة ملف السجل والذي يعرض لك الاتصالات بين **NetScanTools** وخادم**SMTP** .

NetScanTools Pro's Email Relay Testing Tool يسمح لك بأداء اختبار تتابع (**relay test**) من خلال التواصل مع خادم **SMTP**. يتضمن تقرير السجل الاتصالات بين **NetScanTools** وخادم**SMTP** الهدف.

DNS ENUMERATION 4.8

حتى الآن، لقد ناقشنا مفاهيم التعداد، وكيفية تعداد **NETBIOS**، **SNMP**، **يونيكس / لينكس**، **LDAP**، **NTP**، **SMTP**، وما هي المعلومات التي يمكن الحصول عليها من تلك العمليات التعداد. الآن سوف نناقش تعداد **DNS** والمعلومات التي يمكن الحصول عليها من ذلك.

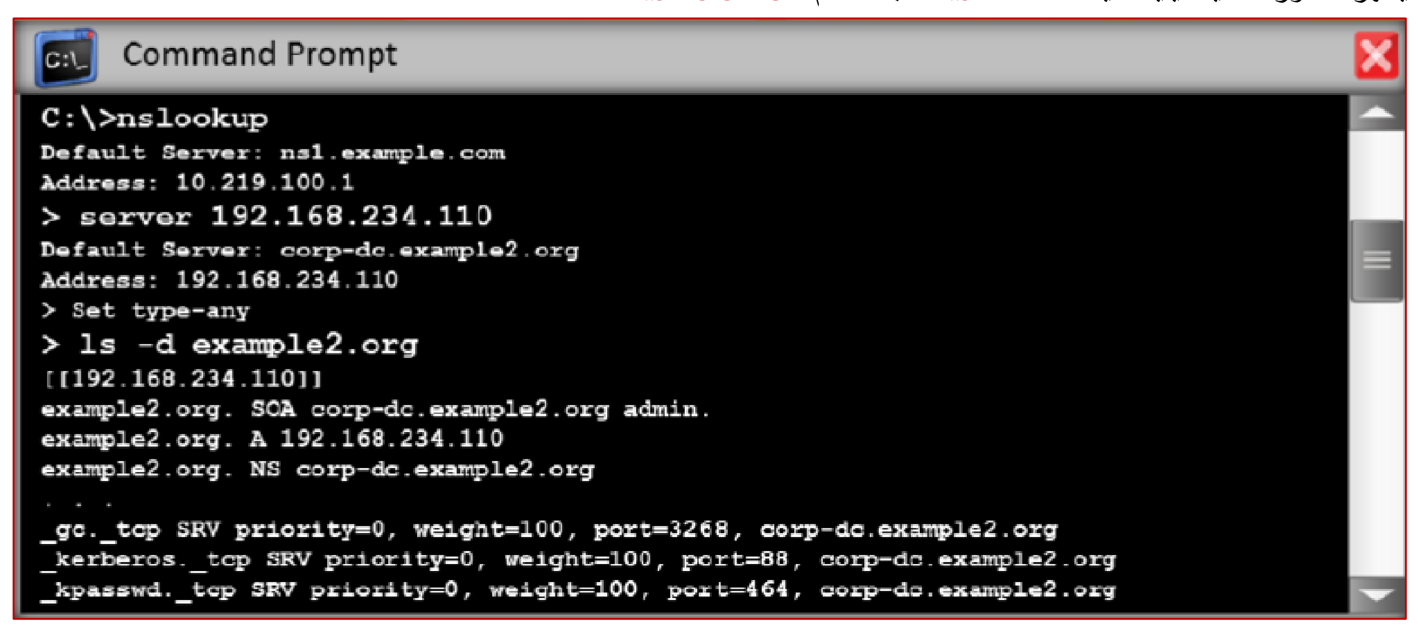
يصف هذا القسم تعداد نقل منطقة **DNS** (***DNS Zone transfer***) والأدوات التي يمكن استخدامها لاستخراج سجلات **DNS** (**DNS record**).

DNS ZONE TRANSFER ENUMERATION USING NSLOOKUP

المهاجم ينفذ تعداد نقل منطقة **DNS** (*DNS Zone Transfer Enumeration*) لتحديد ملقم **DNS** وسجلات المنظمة المستهدفة. من خلال هذه العملية، فان المهاجم يجمع معلومات قيمة عن الشبكة الهدف مثل أسماء ملقم **DNS**، أسماء المضيفين، وأسماء الآلة وأسماء المستخدمين وعناوين **IP** من الأهداف المحتملة. لإجراء تعداد نقل منطقة **DNS**، يمكنك استخدام أدوات مثل **NSLOOKUP**،**DNSstuff** ، وغيرها من الأدوات. هذه الأدوات تمكنك من استخراج نفس المعلومات التي يستخرجها المهاجم من خوادم **DNS** للمنظمة المستهدفة.

لإجراء نقل منطقة **DNS**، فإنك تحتاج إلى إرسال طلب لنقل منطقة إلى ملقم **DNS** والذي يتظاهر بأنه عميل؛ ملقم **DNS** يرسل جزء من قاعدة بياناته كمنطقة لك. قد تحتوي هذه المنطقة على الكثير من المعلومات حول شبكة منطقة **DNS**.

يظهر الصورة التالية كيفية تنفيذ نقل منطقة **DNS** باستخدام **NSLOOKUP**:



4.9 مضادات عملية التعداد ENUMERATION COUNTERMEASURE

حتى الآن، لقد ناقشنا ما هو التعداد، وكيفية أداء أنواع مختلفة من التعداد، ونوع المعلومات التي يمكن للمهاجم استخراجها من خلال عملية التعداد. الآن حان الوقت للنظر في التدابير المضادة التي يمكن أن تساعدك على الحفاظ على المهاجمين بعيدا عن تعداد المعلومات الحساسة عن الشبكة أو المضيف.

يركز هذا القسم على كيفية تجنب تسرب المعلومات من خلال **SNMP**، **DNS**، **SMTP**، **LDAP**، والشركات الصغيرة والمتوسطة.

يمكنك تطبيق التدابير المضادة التالية لمنع تسرب المعلومات من خلال الأنواع المختلفة من التعداد.

التدابير المضادة لتعداد SNMP (SNMP ENUMERATION COUNTERMEASURES):

1- إزالة **SNMP Agent** أو إيقاف تشغيل خدمة **SNMP** من النظام الخاص بك.
2- إذا كان اغلاق خدمة **SNMP** ليست خيارا، فانه يجب عليك تغيير "**public Community name**" الافتراضي.
3- تحديث إصدارات **SNMP** التي لديك إلى **SNMP3**، حيث هذا الإصدار يقوم بتشفير كلمات المرور والرسائل.
4- تنفيذ الخيار الأمني نهج المجموعة (*grouped policy*) والتي تسمى "**Additional restrictions for anonymous connections**".
5- تقييد الوصول إلى **null session pipes**، **null session share**، وفلترة **IPSEC**.
6- منع الوصول إلى المنافذ 161 **TCP / UDP**.
7- لا تقم بتثبيت أدوات إدارة ومراقبة مكونات الويندوز إلا إذا كان ذلك مطلوبا.
8- التشفير أو المصادقة باستخدام **IPSEC**.

التدابير المضادة لتعداد DNS (DNS ENUMERATION COUNTERMEASURES):

1- اعداد كافة ملقمات الاسماء (name server) بعدم السماح للقيام بعملية نقل منطقة DNS الى مضيفين لا يمكن الاعتماد عليهم.
2- التحقق من الإتاحة العامة لملفات المنطقة DNS لملقم DNS، والتأكد من أن عناوين IP في هذه الملفات لا يتم الرجوع إليها بواسطة أسماء المضيفين غير العامة.
3- تأكد من أن ملفات المنطقة DNS لا تحتوي على HINFO أو أي سجلات أخرى.
4- توفير تفاصيل الاتصال لمسئولي الشبكة في مركز قواعد بيانات لشبكة المعلومات. وهذا يساعد على تجنب حرب الاتصال أو هجمات الهندسة الاجتماعية.
5- تقليم ملفات المنطقة DNS لمنع الكشف عن المعلومات غير الضرورية.

التدابير المضادة لتعداد SMTP (SMTP ENUMERATION COUNTERMEASURES):

نقوم بإعداد خادم SMPT كالاتى:

1- تجاهل رسائل البريد الإلكتروني إلى المستلمين الغير معروفين.
2- استجابات البريد لا تشمل معلومات خادم البريد الحساسة والمعلومات عن المضيف المحلي.
3- تعطيل ميزة ترحيل فتح رسائل البريد الإلكتروني. تجاهل رسائل البريد إلى المستلمين الغير معروفين من قبل اعداد ملقمات SMTP.

التدابير المضادة لتعداد LDAP (LDAP ENUMERATION COUNTERMEASURES):

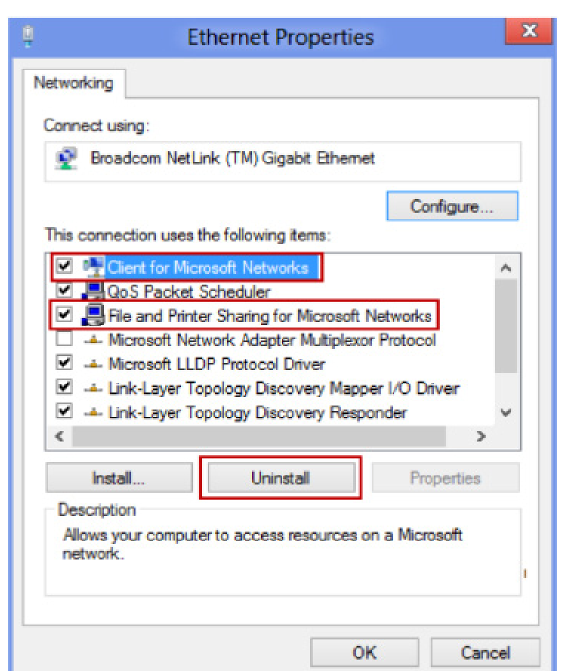
1- استخدام NTLM أو المصادقة الأساسية (Basic Authentication) لتقييد الوصول إلى المستخدمين المعروفة فقط.
2- افتراضيا، حركة المرور LDAP غير مشفره؛ لذلك يفضل استخدام تكنولوجيا SSL لتشفير حركة المرور.
3- حدد اسم مستخدم مختلف عن عنوان البريد الإلكتروني الخاص بك وتمكين تأمين الحساب.

التدابير المضادة لتعداد SMB (SMB ENUMERATION COUNTERMEASURES):

الخدمات المشتركة الشائعة أو الخدمات الأخرى الغير مستخدمة قد تكون المداخل للمهاجمين لاقتحام أمن النظام. ولذلك، يجب تعطيل هذه الخدمات لتجنب تسرب المعلومات أو أنواع أخرى من الهجمات. إذا لم تقم بتعطيل هذه الخدمات، فإنها سوف تكون عرضة لعملية التعداد. بروتوكول Server Message Block (SMB) هي خدمة تهدف إلى توفير الوصول المشترك إلى الملفات والمنافذ التسلسلية، والطابعات، والاتصالات بين العقد على الشبكة. إذا تم تشغيل هذه الخدمة على الشبكة الخاصة بك، فإنك سوف تكون في خطر كبير من الحصول على هجوم. لذلك، يجب عليك تعطيله إن لم يكن ضروريا، لمنع التعداد.

الخطوات التالية لتعطيل SMB:

1- انتقل إلى Etherent Proprieties.
2- نحدد على الخانات Client for Microsoft Networks و File and Printer Sharing for Microsoft Networks.
3- ننقر فوق إلغاء التثبيت.
4- نتبع خطوات الإلغاء.



يصف هذا القسم أهمية التعداد بالنسبة لمختبري الاختراق، الخطوات التي يتبعها مختبري الاختراق، والأدوات التي يمكن استخدامها لإجراء اختبار الاختراق.

من خلال عملية التعداد، فأن المهاجم يقوم بجمع المعلومات الحساسة عن المنظمات إذا كان الأمن غير قوي. ينتج عن هذا استخدام تلك المعلومات الحساسة لاختراق وكسر شبكة المنظمة. إذا قام مهاجم باختراق المنظمة، فأن المنظمة من المحتمل أن تواجه خسائر كبيرة من حيث المعلومات، والخدمة، أو التمويل. لذا، لتجنب هذه الأنواع من الهجمات، فيجب على كل منظمة اختبار أمنها. اختبار أمن منظمة ضد التعداد قانونيا ويسمى تعداد مختبري الاختراق. يجرى عملية تعداد مختبري الاختراق مع مساعدة من البيانات التي تم جمعها في مرحلة الاستطلاع.

بمثابة مختبر الاختراق، فان إجراء تعداد مختبر الاختراق للتحقق ما إذا كانت الشبكة الهدف تكشف عن أي معلومات حساسة يمكن أن تساعد المهاجمين لتنفيذ الهجوم المخطط له جيدا. تنطبق على جميع أنواع تقنيات التعداد لجمع المعلومات الحساسة مثل حسابات المستخدمين، عنوان**IP** ، اتصالات البريد الإلكتروني، **DNS**، موارد الشبكة والمشاركات، معلومات عن التطبيقات، وأكثر من ذلك بكثير. هذا يساعدك في اكتشاف أكبر قدر من المعلومات الممكنة بشأن الهدف. هذا يساعدك على تحديد نقاط الضعف في أمن المنظمة الهدف.

كمختبر اختراق يجب عليك إجراء جميع الأساليب الممكنة من عمليات التعداد، لتعداد أكبر قدر من المعلومات الممكنة حول الهدف. لضمان النطاق الكامل للاختبار، وينقسم الاختبار إلى خطوات التعداد. ويشمل اختبار الاختراق هذا سلسلة من الخطوات للحصول على المعلومات المطلوبة.

START
- Find the network range → Use tools such as WhoIs Lookup
- Calculate the subnet mask → Use Subnet Mask Calculators
- Undergo host discovery → Use tools such as Nmap (nmap - sP <network-range>)
- Perform port scanning → Use tools such as Nmap (nmap -sS <network-range>)

1- البحث في نطاق الشبكة Find the network range

إذا كنت ترغب في اقتحام شبكة المؤسسة، يجب أن نعرف مدى الشبكة الأولى. هذا هو لأنه إذا كنت تعرف نطاق الشبكة، ثم يمكنك إخفاء نفسك كمستخدم يقع ضمن هذا النطاق ومن ثم محاولة الوصول إلى الشبكة. وبالتالي فإن الخطوة الأولى في التعداد مختبري الاختراق هو الحصول على معلومات حول نطاق الشبكة. يمكنك العثور على نطاق الشبكة للمنظمة الهدف مع مساعدة من الأدوات مثل بحث **Whois**.

2- حساب قناع الشبكة Calculate the subnet mask

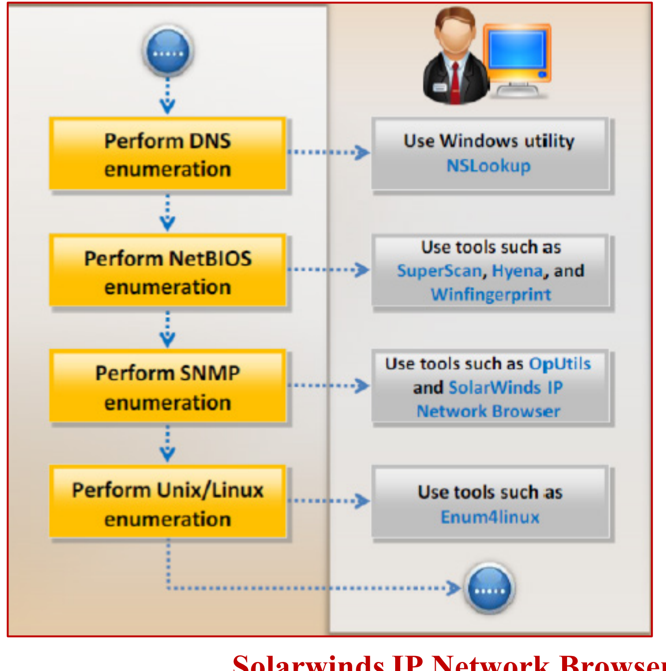
عندما تجد نطاق الشبكة للشبكة المستهدفة، ثم تقوم بحساب قناع الشبكة الفرعية (**subnet mask**) اللازمة لنطاق IP باستخدام أدوات مثل **Subnet Mask Calculator**. فانه يمكنك استخدام قناع الشبكة الفرعية المحسوب كمدخل لكثير من اكتساح بينج (**ping swap**) وأدوات فحص المنفذ لمزيد من التعداد، والذي يتضمن اكتشاف المضيفين والمنافذ المفتوحة.

3- الخضوع لاكتشاف المضيف Undergo host discovery

العثور على خوادم هامة متصلة بشبكة الإنترنت باستخدام أدوات مثل **Nmap**. بناء الجملة في **Nmap** للعثور على الخوادم المتصلة بالإنترنت هي كما يلي:(**nmap -sP <network-range>**). في مكان نطاق الشبكة(**network-range**)، ندخل قيمة نطاق الشبكة التي تم الحصول عليها في الخطوة الأولى.

4- إجراء فحص المنافذ Perform port scanning

من المهم جدا اكتشاف المنافذ المفتوحة وإغلاقها إذا لم تكن تحتاجها. ذلك لأن المنافذ المفتوحة هي المداخل للمهاجمين لاقتحام المحيط الأمني للهدف. وبالتالي، تنفيذ فحص المنافذ للتحقق من المنافذ المفتوحة على العقد. هذا يمكن أن يتحقق مع مساعدة من الأدوات مثل **Nmap**.



5- إجراء التعداد DNS

تنفيذ تعداد DNS لتحديد موقع كافة ملقمات DNS وسجلاتها. توفر خوادم DNS المعلومات مثل أسماء النظام، أسماء المستخدمين وعناوين IP، وما إلى ذلك. يمكنك استخراج كافة هذه المعلومات بمساعدة من الأداة **NSLOOKUP**.

6- إجراء تعداد NETBIOS

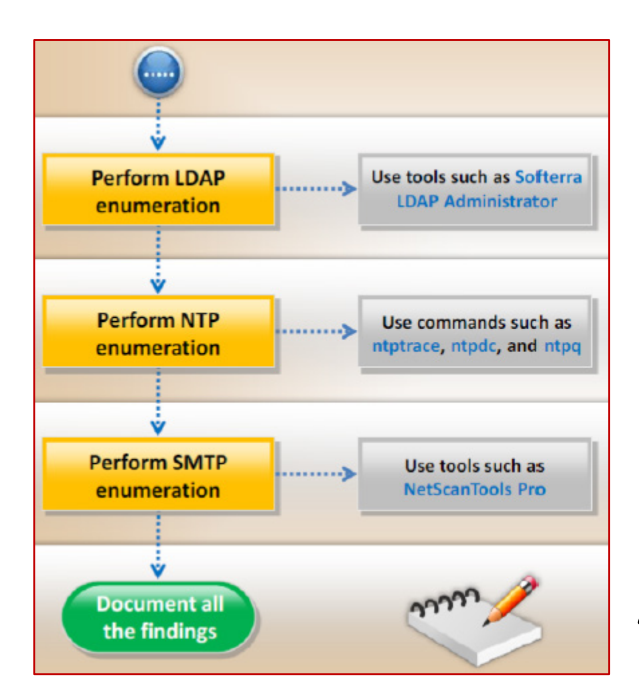
أداء تعداد ***NETBIOS*** لتحديد أجهزة الشبكة عبر **TCP/IP** والحصول على قائمة من أجهزة الكمبيوتر التي تنتمي إلى الدومين، قائمة المشاركات الفردية على المضيفين، والسياسات وكلمات السر. يمكنك تنفيذ تعداد **NETBIOS** بمساعدة من الأدوات مثل **Superscan**، **Hyena**، و**WinFingerprint**.

7- إجراء التعداد SNMP

أداء تعداد **SNMP** عن طريق الاستعلام عن خادم **SNMP** في الشبكة. قد يكشف خادم **SNMP** المعلومات حول حسابات المستخدمين والأجهزة. يمكنك تنفيذ تعداد **SNMP** باستخدام أدوات مثل **OpUtils** و**Solarwinds IP Network Browser**.

8- تنفيذ تعداد يونيكس / لينكس

أداء تعداد يونيكس / لينكس باستخدام أدوات مثل **Enum4linux**. يمكنك استخدام الأوامر مثل **Showmount**، **Finger**، **rpcinfo** (**RPC**)، و **rpcclient** وغيرها من الأدوات. وذلك لتعداد موارد شبكة يونكس.



9- إجراء التعداد LDAP

تنفيذ تعداد **LDAP** بواسطة الاستعلام عن خدمة **LDAP**. عن طريق الاستعلام عن خدمة LDAP يمكنك تعداد أسماء المستخدم الصالح وتفاصيل الإدارات، وتفاصيل العنوان. يمكنك استخدام هذه المعلومات لأداء الهندسة الاجتماعية وأنواع أخرى من الهجمات. يمكنك تنفيذ تعداد **LDAP** باستخدام أدوات مثل مدير **Softerra LDAP**.

10- إجراء التعداد NTP

أداء تعداد **NTP** لاستخراج المعلومات مثل المضيف المتصل بخادم **NTP**، عنوان **IP** للعميل، ونظام التشغيل أنظمة العميل، وما إلى ذلك يمكنك الحصول على هذه المعلومات بمساعدة من الأوامر مثل **ntptrace**، **ntpdc**، و**ntpq**.

11- إجراء التعداد SMTP

تنفيذ تعداد **SMTP** لتحديد المستخدمين الصالحة على الملقم **SMTP**. يمكنك استخدام أدوات مثل **NetScanTools pro** للاستعلام عن خادم **SMTP** لهذه المعلومات.

12- توثيق جميع النتائج

الخطوة الأخيرة في كل اختبار الاختراق هو توثيق جميع النتائج التي تم الحصول عليها أثناء الاختبار. يجب تحليل واقتراح التدابير المضادة للعميل الخاص بك لتحسين أمنهم.

الان والحمد لله قد انتهينا من الوحدة الرابعة. حيث تحدثنا في الوحدة الأربع عن عمليات جمع المعلومات التي تلخصت في مراحل Footprinting وscanning وenumeration. الان سوف ننتقل الى مرحله أخرى كما سوف يسرد في الوحدة القادمة بإذن الله.

د. محمد صبحي طيبه (01009943027)